Intellectual Property Law in Cyberspace

Second Edition

2014 Cumulative Supplement

Chapter 13: Intellectual Property Issues Raised by Email

G. Peter Albert, Jr.

and

American

Intellectual Property Law

Association

AIPLA

American
Intellectual Property Law
Association
Arlington, VA

Bloomberg BNA

Bloomberg BNA, Arlington,VA

Library of Congress Cataloging-in-Publication Data

Albert, G. Peter, 1964–
Intellectual property law in cyberspace / G. Peter Albert, Jr. – 2nd ed.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-57018-753-7 (alk. paper)
1. Industrial property–United States. 2. Computer networks–Law and legislation–United States. 3. Internet 4. Copyright and electronic data processing–United States. I. Title.
KF3095.A77 2011
346.7304'8–dc23

2011040494

Published by Bloomberg BNA
1801 S. Bell Street, Arlington, VA 22202
bna.com/bnabooks

ISBN 978-1-61746-491-1
Printed in the United States of America

13

Intellectual Property Issues Raised by Email

Michael B. Smith
Law Office of Michael B. Smith
Natick, Massachusetts

Sara Anne Hook
Indiana University School of Informatics and Computing
Indianapolis, Indiana

Aly Dossa
Osha Liang LLP
Houston, Texas

II. ISSUES ARISING OUT OF PERMISSIBLE USE OF EMAIL

A. Privacy/Confidentiality

[Add the following at the end of the section.]

Several bills introduced in Congress over the last two years reflect the public's continued concerns over what should be considered permissible with respect to accessing a person's email and other electronic

information. H.R. 537, the Social Networking Online Protection Act,[1] reminiscent of legislation with the same title that was proposed in 2012, responds to the growing trend of employer requests for information that would allow access to personal social media or private email accounts, including as part of the hiring process or as a basis for adverse action if an employee or applicant refuses to provide this information.[2] The bill summary notes that the Act

> [p]rohibits employers from: (1) requiring or requesting that an employee or applicant for employment provide a user name, password, or any other means for accessing a private email account or personal account on a social networking Web site; or (2) discharging, disciplining, discriminating against, denying employment or promotion to, or threatening to take any such action against any employee or applicant who refuses to provide such information, files a compliant [*sic*] or institutes a proceeding under this Act, or testifies in any such proceeding.[3]

An additional provision in the proposed legislation would amend the Higher Education Act of 1965 and the Elementary and Secondary Education Act of 1965 "to prohibit certain institutions of higher education and local educational agencies from requesting such password or account information from students or potential students."[4] The bill also forbids a variety of retaliatory actions against employees, applicants, students and potential students who refuse to provide the information or who seek redress through filing a complaint, instituting a proceeding, or testifying in a proceeding.[5] Both civil penalties and injunctive relief would be available.[6]

Another piece of legislation, introduced in May 2013, responds directly to the privacy concerns with email communications that are provided through or stored by third-party and cloud computing service providers. H.R. 1852, the Email Privacy Act,[7] would "amend title 18, United States Code, to update the privacy protections for electronic communications information that is stored by third-party service providers in order to protect consumer privacy interests while meeting law enforcement needs, and for other purposes."[8] Among the various provisions in the proposed legislation are confidentiality of electronic communications, elimination of the 180-day rule, requirements for search warrants, required

---

[1] *See* Summary: H.R.537—113th Congress (2013-2014), *available at* https://www.congress.gov/bill/113th-congress/house-bill/537.

[2] *See* Text: H.R.537—113th Congress (2013-2014), *available at* https://www.congress.gov/bill/113th-congress/house-bill/537/text.

[3] Summary: H.R.537.

[4] *Id.*

[5] Text: H.R.537 §2(a)(2), §4(a)(2).

[6] *Id.* §2(b)(1), (b)(2).

[7] *See* Summary: H.R.1852—113th Congress (2013–2014), *available at* https://www.congress.gov/bill/113th-congress/house-bill/1852/.

[8] Text: H.R.1852—113th Congress (2013-2014), *available at* https://www.congress.gov/bill/113th-congress/house-bill/1852/text.

disclosure of customer records, delay of notification, evaluation by the government accountability office and rules of construction.[9]

Clearly a response to the recent events surrounding the disclosures from Edward Snowden about NSA surveillance, H.R. 2399 Limiting Internet and Blanket Electronic Review of Telecommunications and Email Act, or LIBERT-E Act,[10] was introduced on June 17, 2013. The bill is intended to "prevent the mass collection of records of innocent Americans under section 501 of the Foreign Intelligence Surveillance Act of 1978, as amended by section 215 of the USA PATRIOT Act, and to provide for greater accountability and transparency in the implementation of the USA PATRIOT Act and the Foreign Intelligence Surveillance Act of 1978."[11] Among the many provisions outlined in the legislation are: amending Section 501 of the Foreign Intelligence Surveillance Act of 1978[12] with respect to access to certain business records for foreign intelligence and international terrorism investigations; amending Section 601 of the Foreign Intelligence Surveillance Act of 1978[13] to provide additional disclosures to Congress and the public; requiring a report on the impact on the privacy of people located in the United States by provisions related to certain business records and targeting of non-United States persons outside of the United States; and a new paragraph added to Section 702(l) of the Foreign Intelligence Surveillance Act of 1978[14] on the forms of assessments and reviews.[15]

The Personal Data Privacy and Security Act of 2014[16] is a far-reaching bill that enhances penalties for identity theft and other violations of data privacy and security, sets requirements for business entities engaging in interstate commerce related to the privacy and security of personally identifiable information, and provides for compliance of the budgetary effects of the Act with the Statutory Pay-As-You-Go Act.[17] In addition, this legislation defines "sensitive personally identifiable information" to include:

> (1) specified combinations of data elements in electronic or digital form, such as an individual's name, home address or telephone number, mother's maiden name, and date of birth; (2) a non-truncated social security

---

[9] *Id.*

[10] *See* Summary: H.R.2399—113th Congress (2013-2014), *available at* https://www.congress.gov/bill/113th-congress/house-bill/2399.

[11] Text: H.R.2399—113th Congress (2013-2014), *available at* https://www.congress.gov/bill/113th-congress/house-bill/2399/text.

[12] 50 U.S.C. §1861.

[13] *Id.* §1871.

[14] *Id.* §1881a.

[15] *Id.* It will be especially interesting to monitor these three pieces of legislation as they move forward and to consider the extent to which email continues to be a major method of communication for employees, companies, law firms, students and citizens and is thus worthy of vigilance in security and privacy practices.

[16] *See* Summary: H.R.3990—113th Congress (2013-2014), *available at* https://www.congress.gov/bill/113th-congress/house-bill/3990; *see also* Summary: S.1897—113th Congress (2013-2014), *available at* https://www.congress.gov/bill/113th-congress/senate-bill/1897.

[17] *See* Pub. L. No. 111-139, 124 Stat. 8 (Feb. 12, 2010).

> number, driver's license number, passport number, or government-issued unique identification number; (3) unique biometric data; (4) a unique account identifier; and (5) any security code, access code, password, or secure code that could be used to generate such codes or passwords.[18]

Although email is not mentioned specifically in the definition of "sensitive personally identifiable information," it is discussed in the provisions of the legislation that address the requirements for notification in the event of a breach:

> An agency or business entity shall be in compliance with section 211 if it provides the following:
>
> (1) Individual notice.—Notice to individuals by one of the following means:
>
> (A) Written notification to the last known home mailing address of the individual in the records of the agency or business entity.
>
> (B) Telephone notice to the individual personally.
>
> (C) E-mail notice, if the individual has consented to receive such notice and the notice is consistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001).[19]

A bill with similar provisions that was introduced in February 2014 is S.1995, the Personal Data Protection Act and Breach Accountability Act of 2014.[20] In addition to the contents of H.R.3990 and S.1897, the bill adds Title III, Access to and Use of Commercial Data. Among the interesting provisions of this bill are a number of requirements for federal agencies that could serve as best practices when dealing with contractors, third-party business entities, and data brokers:

> Requires federal agencies to: (1) evaluate and audit the information security practices of contractors or third party business entities that support the information systems or operations of such agencies involving sensitive personally identifiable information, and (2) ensure remedial action to address any significant deficiencies.
>
> Requires federal agencies to conduct a privacy impact assessment before purchasing or subscribing to personally identifiable information from a data broker. Requires the Comptroller General to report on federal agency adherence to key privacy principles in using data brokers of commercial databases containing sensitive personally identifiable information.[21]

---

[18] Summary: H.R.3990.

[19] Text: H.R.3990 $213(1)(A)–(C).

[20] *See* Summary: S.1995—113th Congress (2013-2014), *available at* https://www.congress.gov/bill/113th-congress/senate-bill/1995.

[21] *Id.*

A more narrowly tailored bill, H.R.4157, the Farmer Identity Protection Act,[22] indicates that a wide variety of citizens have specific concerns about privacy, including the privacy of their email addresses. The Act, introduced in March 2014, would prohibit:

> the Environmental Protection Agency (EPA), or any EPA contractor or cooperator, from disclosing the information of any owner, operator, or employee of a livestock operation provided to EPA by a livestock producer or a state agency in accordance with the Federal Water Pollution Control Act (commonly known as the Clean Water Act) or any other law, including: (1) names; (2) telephone numbers; (3) e-mail addresses; (4) physical addresses; (5) global positioning system coordinates; or (6) other information regarding the location of the owner, operator, livestock, or employee.[23]

1. Work vs. Home

[Add the following at the end of the section.]

A new book by Nelson, Ries, and Simek provides a chapter on email security, along with substantial information on securing all types of devices.[24]

A number of recent articles should heighten an attorney's awareness of the significant risks to information security and confidentiality posed by the use of mobile devices, which are typically the means by which email is exchanged. Often, the issue is not the technology itself, but human behavior that causes mobile devices to be lost or stolen at alarming rates. Law firms are only beginning to grapple with some of these issues.[25] Nelson and Simek, who are experts in information security and privacy matters, provide a number of helpful recommendations for security when using smartphones, with a reminder that attorneys have an ethical obligation to protect confidential client information.[26] They also advise attorneys to be aware of the changes to the ABA Model Rules of Professional Conduct because under the revisions to the Rules (as part of the Ethics 20/20 project), attorneys are now required to use technology competently and to assess the risks of any particular technology and the sensitivity of the data being handled as it relates to the measures being taken to secure the data.[27] An article by Nelson and Simek covers how to securely delete

---

[22] *See* Summary: H.R.4157—113th Congress (2013-2014), *available at* https://www.congress.gov/bill/113th-congress/house-bill/4157.

[23] *Id.*; *see also* Farmer Identity Protection Act, Summary: S.1343—113th Congress (2013–2014), *available at* https://www.congress.gov/bill/113th-congress/senate-bill/1343.

[24] Sharon D. Nelson, David G. Ries & John W. Simek, Locked Down: Information Security for Lawyers (ABA 2012).

[25] *See* Melody Finnemore, *The Data Dilemma: Law Firms Strive to Strengthen E-Security as Potential Threats Continue to Arise*, 77 Or. St. B. Bull. 27 (Oct. 2012).

[26] Sharon D. Nelson & John W. Simek, *Our Top 16 Security Tips for Smartphones* (Sensei Enterprises 2012), *available at* http://senseienterprisesinc.squarespace.com/storage/articles/Our%20Top%2016%20Security%20Tips%20for%20Smartphones.pdf.

[27] *Id.* at 4.

data from mobile devices.[28] One of the preferred ways to ensure the security and confidentiality of email is to use proper encryption methods. A recent article by Ries and Simek discusses how encryption works and provides suggestions for securing laptops and portable media, smartphones and tablets, wireless networks and email.[29]

Where the line is really beginning to blur between work and home is the growing trend towards employees using their personal devices (smartphone, tablets, laptops) for employment-related activities, which is now referred to as Bring Your Own Device (BYOD). BYOD is not really a new concept, because many organizations have allowed employees to work from home for years, providing them with remote access to whatever software and systems were needed, including email. The new twist is that employees are now connecting through tablets and iPhones, many of which are owned by the employees. Some commentators have suggested that this phenomenon should be referred to as BYOT—Bring Your Own Technology—because employees *also* are choosing the outside software and apps that they want to download onto their devices, not all of which provide sufficient security features. Whether referred to as BYOD or BYOT, this trend presents a number of risks to lawyers and law firms as well as to the clients that they represent.

Issues related to BYOD are expected to multiply, especially if employers begin to require their employees to pay for their own devices and for the technology to support them. Certainly, this saves the employer from the expense of purchasing the devices as well as the cost of robust, centralized IT support. If the employer provides a stipend to purchase devices or network services, this further complicates the issue of who owns or controls the device, how it is used, and its contents (see below). In fact, recent commentators suggest that in the future, more employers may choose to provide employees with a stipend towards the purchase of these devices and for network services.

Allowing or mandating that employees use personal devices means that business and personal data are now jumbled together and raises the question of who owns the information.[30] Although most commentators urge the development of a BYOD policy, Tigue cautions that "[a] comprehensive BYOD policy does not guarantee that an employer can effectively control corporate data that has been commingled with personal records on devices that the company does not truly control."[31] Believing that "BYOD polices have little practical effect" and may even hamper the discovery process, she suggests that the best policy for the employer may be to prohibit the use of personal devices for work purposes and to in-

---

[28] Sharon D. Nelson & John W. Simek, *Securely Deleting Data from Mobile Devices* (Sensei Enterprises 2012), *available at* http://www.slaw.ca/2012/07/30/securely-deleting-data-from-mobile-devices/.

[29] David G. Ries & John W. Simek, *Encryption Made Easy for Lawyers*, 56 (8) Res Gestae 24–31 (Apr. 2013).

[30] *See* Tara Tighe, *Mobile Devices Blur Lines Between Business and Personal Data*, 16 Lawyers J. 7 (Jan. 24, 2014).

[31] *Id.* at 7.

form employees that they will be personally liable if company policies are violated or corporate data stored on a personal device is lost, suppressed or misused.[32]

BYOD raises concerns about privacy rights over personal information, especially for employees in the public sector. Heaton notes that while public-sector employees do not have a right to disclose confidential government information, "an agency has to be extremely careful to segregate private and public information on a device" so that only government data is monitored.[33] Among the solutions offered for employers are to allow employees to review but not store government data on their devices; to draft carefully worded policies that address privacy and First Amendment issues; to segregate data; to use search-access agreements and financial disclaimers about purchasing, upgrading or paying for access services; and to require employees to use passwords on personal devices and provide those passwords to the employer.[34]

As an example of the pervasiveness of these issues, and the myriad ways in which they can be addressed, H.R.3520, the Exempt Organization Simplification and Taxpayer Protection Act of 2013[35]—primarily intended to streamline and clarify the process for entities to apply to operate as tax-exempt social welfare organizations—contains the requirement that "[n]o officer or employee of the Internal Revenue Service may use a personal email account to conduct any official business of the Government."[36]

Murphy discusses the impact of the increasing use of mobile devices by lawyers and law firm employees.[37] He describes how this blurring of personal and business computing is creating special challenges for law firms and their IT departments, including security as an afterthought, data contamination, mobile malware, phishing attacks that can bypass network defenses, lost devices, and risky file sharing.[38] He advocates using a security file-sharing solution which can shield confidential data from unauthorized access and from malware that may have infected other files on the device.[39]

Beck notes that the data being stored on mobile devices continues to grow because of email messages and attachments, text messages and other instant messaging services, app data, multimedia files and metadata.[40]

---

[32] *Id.* at 8.

[33] Brian Heaton, *The Legal Implications of BYOD*, Gov't Tech. (Oct. 7, 2013), *available at* http://www.govtech.com/data/The-Legal-Implications-of-BYOD.html (last visited June 19, 2014).

[34] *Id.*

[35] *See* Summary: H.R.3520—113th Congress (2013-2014), *available at* https://www.congress.gov/bill/113th-congress/house-bill/3520.

[36] Text: H.R.3520—113th Congress (2013-2014) §6, *available at* https://www.congress.gov/bill/113th-congress/house-bill/3520/text.

[37] Coleman Murphy, *Contain Yourself: Top Five Ways to Protect Mobile Data*, Peer to Peer (Mar. 2013), at 16–19.

[38] *Id.* at 17–19.

[39] *Id.* at 19.

[40] David Beck, *Mobile Device Management: The Missing Piece of the Puzzle*, Peer to Peer (Sept. 2012), at 80–88.

He notes that proper mobile device management (MDM) begins with information governance, including policies and standards.[41] Essential MDM technical controls covered in his article include asset management, configuration management, encryption and remote secure wipe.[42]

Not only are mobile devices prone to being lost or stolen, but people also continue to fall victim to the tactics of social engineering, which Carlson and Wolf define as manipulating people into disclosing information or performing tasks. Social engineering can present risks to the security of email if people can be inveigled to reveal confidential information, such as user identification and passwords. Statistics indicate that people who use their smartphones for work have inconsistent security habits, including not protecting their phones with passwords, using unsecure Wi-Fi networks, and not disabling Bluetooth discoverable modes.[43]

The fact that the device being used is a personal rather than an employer-provided device may mean that people are less vigilant about potential threats and more casual about observing and using proper security protocols and tools.[44]

Nelson and Simek report that not only are law firms often the victims of security breaches, but that often lawyers in those law firms are not even aware that there has been a breach.[45] Nelson and Simek also reveal that these firms often fail to notify clients of a breach.[46] They cite a survey conducted by the ABA's Legal Technology Resource Center that found that "15 percent of survey respondents had experienced a security breach, and respondents of mid-size firms (10–99 attorneys) were most likely to know about the breach."[47] The authors relate that "[t]he survey highlighted the increased risks from bring-your-own-device policies which allow attorneys to access firm networks through their smartphones, tablets or other devices. The report found that '34 percent of respondents reported that their firms allowed them to connect their personal mobile devices to the network without restrictions.'"[48]

Carlson and Wolf's article discusses the importance of training lawyers and their staff members about information security threats which can be helpful for clients as well. In terms of keeping mobile employees

---

[41] *Id.* at 81.

[42] *Id.* at 81–82. *See also* Paula Skokowski, *Stop, Thief: Protecting Legal Documents in a Mobile World*, Peer to Peer (Sept. 2012), at 84–88; Charles Magliato, *Making BYOD Work for Legal*, Peer to Peer (Sept. 2012), at 20–24.

[43] KMWorld Staff, *The Truth About BYOD*, KM World (Apr. 29, 2013), at 1–2, *available at* http://www.kmworld.com/Articles/News/News-Analysis/The-truth-about-BYOD-89090.aspx.

[44] Adam Carlson & Matt Wolf, *Train to Strengthen Security's "Weakest Link,"* Peer to Peer (Sept. 2012), at 52–56.

[45] Sharon Nelson & John Simek, *70% of Large Firm Lawyers Don't Know If Their Firm Has Been Breached*, Legal by the Bay (Mar. 4, 2014), *available at* http://blog.sfbar.org/2014/03/04/70-of-large-firm-lawyers-dont-know-if-their-firm-has-been-breached/ (last visited June 18, 2014).

[46] *Id.*

[47] *Id.*

[48] *Id.*

and their data safe, Nabavi provides a number of best practices for keeping IT secure, whether it is mobile or stationary[49] and DeSot recommends building a "culture of security."[50] Hilal provides a number of practical suggestions for implementing and managing BYOD that are valuable for both law firms and their clients.[51] He identifies the two basic models of corporate-owned and employee-owned BYOD and variations of each of these models and notes that an organization must understand its needs and provide clarity to its employees in order to ensure that a BYOD program is successful.[52]

Although there may be cost savings to the employer, Hilal suggests that companies also need to consider device costs to employees as well as costs for voice and data, an IT helpdesk, mobile development, and mobile management.[53] Employers also must be vigilant to ensure an enterprise-wide security strategy that takes into account access through multiple platforms and limited control of applications that may include malicious software.[54]

Likewise, Brown offers a number of suggestions for developing a BYOD strategy.[55] Among his recommendations are adopting a standardized roster of acceptable devices, avoiding devices that are "jailbroken" (*i.e.*, "modified to remove the controls set by the original manufacture"), establishing control through password or pin code policies, adopting some level of encryption, regulating the apps installed by users (especially apps for personal use), and implementing acceptable use policies, Mobile Device Management (MDM) technologies, and strong security controls on the devices.[56] He also reports that productivity is a key concern, especially among the corporate and law firm customers that are members of his company's strategic advisory board.[57]

Special considerations are needed with respect to electronic discovery, not only for the law firm's employees who are working on a case, but particularly related to the lawyer's responsibilities in overseeing the client so that proper collection and preservation procedures and litigation holds are communicated to the client's constituents and are being followed. One issue that is likely to have significant implications is the ESI (Electronically Stored Information) that is available on personal devices and that was communicated through personal email accounts. For

---

[49] Reza Nabavi, *Keep Mobile Workers and Their Data Safe*, Peer to Peer (Sept. 2012), at 26–27.

[50] Tom DeSot, *Build a "Culture of Security,"* Peer to Peer (Sept. 2012), at 28.

[51] Sameer Hilal, *You're Invited to a Device Potluck: Exploring and Managing BYOD*, Peer to Peer (Dec. 2013), at 16–18, *available at* http://read.uberflip.com/i/230349/14.

[52] *Id.* at 16–17.

[53] *Id.* at 17–18.

[54] *Id.* at 18.

[55] Matthew Brown, *BYOD: Taking the Workplace Mobile*, Metropolitan Corporate Counsel (Aug. 22, 2013), at 24, *available at* http://www.metrocorpcounsel.com/articles/25080/byod-taking-workplace-mobile (last visited June 19, 2014).

[56] *Id.*

[57] *Id.*

example, in *Puerto Rico Telephone Co. v. San Juan Cable LLC*,[58] the court determined that the duty to preserve extended to the personal email accounts of a company's former officers, although the court declined a request for sanctions based on an absence of bad faith and failure to show prejudice. Cornwell outlines a number of reasons for the risks of spoliation when using a BYOD strategy.[59] Among the risks he identifies are the movement of data from a company's network to personal devices, especially from smaller companies that do not have a high level of security and controls; angry former or terminated employees who may take company data with them; and overtime related to BYOD, resulting in wage and hour claims, if employees are expected to check and respond to email outside of normal work hours.[60] Among the strategies he suggests to mitigate these risks are allowing "read only" access outside of the company's firewall, the ability to wipe company data from devices remotely, setting up BYOD policies, and establishing a model for handling electronic discovery in the event of litigation.[61]

2. Document Retention Policies

[Add the following at the end of the section.]

A recent article by Nelson and Simek outlines a number of polices and plans that firms should have in place to deal with the vast amount of electronic information that is being generated by employees using a variety of devices and social media sites.[62] These same suggestions seem appropriate for any corporation or organization and the authors also note the importance of annual training as a way to reinforce these policies and plans. Among the policies that the authors advocate for law firms that encompass email and other popular forms of electronic communication and that pose risks to client confidentiality are an electronic communications and Internet use policy, a social media policy, a document retention policy, a secure password policy, an equipment disposal policy, and policies for mobile security.

The technology plans that Nelson and Simek consider essential for law firms are an incident response plan, a disaster recovery plan, and a litigation hold plan. The authors note that "[t]hese policies and plans are an integral part of risk management and ensuring business continuity, two things near and dear to the heart of all lawyers."[63] Drawing on the work of Nelson and Simek, Kerschberg also discusses why companies should

---

[58] No. 11-2135 (GAG/BJM), 2013 WL 5533711 (D.P.R. Oct. 7, 2013).

[59] Ted Cornwell, *'Spoliation' Among Legal Risks in a BYOD World*, National Mortgage News (Dec. 2, 2013), at 6.

[60] *Id.*

[61] *Id.*

[62] Sharon D. Nelson & John W. Simek, *Essential Law Firm Technology Policies and Plans* (Sensei Enterprises 2012), *available at* http://www.senseient.com/articles/pdf/Essential_Law_Firm_Policies_and_Plans.pdf (last visited June 28, 2012).

[63] *Id.* at 5.

have robust social media policies and a secure and reliable method for archiving information generated through social media, especially since it is discoverable in litigation.[64]

One of the most important ways to help clients is to make sure that they have a comprehensive document retention policy that is being used on a regular and consistent basis. On the flip side, one of the worst things that a client can do is to suddenly begin using a document retention policy, especially when it appears that certain electronically stored information that might be relevant to impending litigation has been selectively targeted for disposal. Such was the behavior exhibited by Rambus, resulting in a finding of bad faith and with an appropriate sanction being to declare that the patents-in-suit were unenforceable against Micron.[65] Among the four main categories of facts that supported the finding of bad faith were:

> 1) facts that show that the plaintiff's document retention policy was adopted only as a weapon for litigation; 2) facts that show that the plaintiff's document retention policy was selectively executed, with suspicious documents discarded; 3) facts that show that the plaintiff knew of the impropriety of the document retention policy, minimizing discussion thereof via email, and; 4) plaintiff's litigation misconduct, and misrepresentations in depositions about the number of "shred days."[66]

In a similar case involving Rambus and SK Hynix, the court found that Rambus had committed spoliation, but adjusted the royalty rate as its sanction.[67] In a more recent case, the court awarded a monetary sanction of $250,000,000, which would be applied as a credit against Rambus's more than $300 million judgment against SK Hynix, Inc.[68] The ongoing litigation between Rambus and its competitors not only provides considerable insight into various steps in the electronic discovery process

---

[64]Ben Kerschberg, *Managing Information Risk and Archiving Social Media*, Forbes (9/28/2011), *available at* http://www.forbes.com/sites/benkerschberg/2011/09/28/managing-information-risk-and-archiving-social-media/ (last visited June 28, 2012).

[65]Micron Tech., Inc. v. Rambus Inc., 917 F. Supp. 2d 300 (D. Del. 2013). *See* On Remand, Court Finds Rambus' Spoliation was in Bad Faith and Resulted in Prejudice, Holds Patents-in-Suit Unenforceable Against Micron, *available at* http://www.ediscoverylaw.com/2013/01/articles/case-summaries/on-remand-court-finds-rambus-spoliation-was-in-bad-faith-and-resulted-in-prejudice-holds-patentsinsuit-unenforceable-against-micron/ (K&L Gates January 11, 2013) (last visited June 21, 2013).

[66]*Court Elaborates on the Standard for Bad Faith Spoliation in Patent Infringement Case*, *available at* http://www.krollontrack.com/resource-library/case-law/?caseid=26475 (Kroll Ontrack) (last visited June 21, 2013).

[67]Hynix Semiconductor, Inc. v. Rambus, Inc., No. C-00-20905 RMW (N.D. Cal. Sept. 21, 2012). *See* On Remand, Court Finds Rambus Committed Spoliation, Will Adjust Royalty Rate as Sanction, *available at* http://www.ediscoverylaw.com/2012/09/articles/case-summaries/on-remand-court-finds-rambus-committed-spoliation-will-adjust-royalty-rate-as-sanction/ (K&L Gates September 27, 2012).

[68]SK Hynix, Inc. v. Rambus, Inc., No. C-00-20905 RMW, 2013 WL 1915865 (N.D. Cal. May 8, 2013). *See* Case Update: For Spoliation, Court Orders $250,000,000 "to be applied as a credit against Rambus's [$349 million] judgment against SK Hynix," *available at* http://www.ediscoverylaw.com/2013/05/articles/case-summaries/case-update-for-spoliation-court-orders-250000000-to-be-applied-as-a-credit-against-rambuss-349-million-judgment-against-sk-hynix/ (K&L Gates May 22, 2013) (last visited June 21, 2013).

and the substantial penalties that can be assessed for spoliation, but also points to the importance of having and properly using document retention policies.

Scentsy, Inc. v. B.R. Chase, LLC[69] addresses both inadequate document retention policies and concerns with the litigation hold process, including using oral rather than written litigation holds and inconsistency in handling and storing email and other ESI.[70] Another recent case involving improper handling of email during an electronic discovery process is *Carrillo v. Schneider Logistics, Inc.*[71] In this case, the court ordered monetary sanctions and that an outside vendor be hired after determining that the defendant had failed to comply with its discovery obligations. Among the deficiencies identified were: 1) failing to conduct a "reasonably diligent search,"[72] 2) improperly withholding responsive documents,[73] and 3) failing to take "adequate steps to preserve documents."[74] With the trend towards BYOD, companies will need to be even more thoughtful about how email is handled in all phases of an electronic discovery process as well as policies, procedures and tools for preservation, storage, archiving and destruction of email and other ESI that will now reside on devices that are not directly purchased by or under the control of the employer.

Several recent electronic discovery cases emphasize not only the importance of working with clients to develop and implement an effective records retention policy, but also of ensuring that clients cease their established processes for destroying or otherwise making inaccessible potentially relevant evidence once litigation can be reasonably anticipated.[75]

---

[69] No. 1:11-cv-00249-BLW, 2012 WL 4523112 (D. Idaho Oct. 2, 2012).

[70] *See* Concluding Litigation Hold and Document Retention Policies are "Clearly Unacceptable," Court Allows Depositions to Determine if Spoliation Occurred, *available at* http://www.ediscoverylaw.com/2012/10/articles/case-summaries/concluding-litigation-hold-and-document-retention-policies-are-clearly-unacceptable-court-allows-depositions-to-determine-if-spoliation-occurred (K&L Gates October 16, 2012) (last visited June 21, 2013).

[71] No. CV 11-8557-CAS (DTBx), 2012 WL 4791614 (C.D. Cal. Oct. 5, 2012).

[72] *Id.* at *3.

[73] *Id.* at *5.

[74] *Id.* at *7. *See* For Discovery Violations, Court Orders Retention of Outside Vendor to Collect Responsive Documents, Investigate Possible Spoliation, *available at* http://www.ediscoverylaw.com/2012/11/articles/case-summaries/for-discovery-violations-court-orders-retention-of-outside-vendor-to-collect-responsive-documents-investigate-possible-spoliation/ (K&L Gates November 2, 2012) (last visited June 21, 2013).

[75] Recent cases which specifically discuss email in the context of document retention policies can be found through the K&L Gates E-Discovery Case Database, http://www.ediscoverylaw.com/e-discovery-case-database/ (last visited June 18, 2014). These cases include Ingrid & Isabel, LLC v. Baby Be Mine, LLC, No. 13-cv-01806, 2014 WL 1338480 (N.D. Cal. Apr. 1, 2014); Knickerbocker v. Corinthian Colls., No C12-1142JLR, 2014 WL 1356205 (W.D. Wash. Apr. 7, 2014); Woodlands Dev. LLC v. Regions Bank, 141 So. 3d 357, 2014 WL 2210584 (La. Ct. App. 2014); Hixson v. City of Las Vegas, No. 2:12-cv-00871-RCJ-PAL, 2013 WL 3677203 (D. Nev. July 11, 2013); Herrmann v. Rain Link, Inc., No. 11-1123-RDR, 2013 WL 4028759 (D. Kan. Aug. 7, 2013); PersonalWeb Techs., LLC v. Google Inc., No. C13-01317-EJD (HRL), 2014 WL 580290 (N.D. Cal. Feb. 13, 2014); Zest IP Holdings, LLC v. Implant Direct Mfg., LLC, No. 10-0541-GPC(WVG), 2013 WL 6159177 (S.D. Cal. Nov. 25, 2013).

For example, in response to failure to issue a litigation hold and to monitor preservation, the court in *Zest IP Holdings, LLC v. Implant Direct Mfg., LLC*[76] awarded monetary sanctions and an adverse inference instruction against the defendants.

In *Herrmann v. Rain Link, Inc.*,[77] however, the court declined to sanction the defendants for failing to suspend their routine document retention procedures, even though it resulted in the destruction of documents and ESI, because the plaintiff had not demonstrated that it was prejudiced, or that the defendants acted in bad faith. The court characterized the defendants' failure to suspend their routine practices as negligent as opposed to being done with intent to deprive the plaintiff of evidence.[78]

In a third case, *Sekisui American Corp. v. Hart*,[79] Judge Shira A. Scheindlin (author of the *Zubulake* opinions) reversed an earlier order from the Magistrate Judge wherein he declined to impose spoliation sanctions for the plaintiffs' deletion of ESI that belonged to two important custodians in the case. In her Opinion and Order, she states:

> A decade ago, I issued a series of opinions regarding the scope of a litigant's duty to preserve electronic documents and the consequences of a failure to preserve such documents falling within the scope of that duty. At its simplest, that duty requires a party anticipating litigation to refrain from deleting electronically stored information ("ESI") that may be relevant to that litigation. Such obligation should, at this point, be quite clear—especially to the party planning to sue. Here, I consider the appropriate penalty for a party that—with full knowledge of the likelihood of litigation—intentionally and permanently destroyed the email files of several key players in this action.[80]

Among the deficiencies in Sekisui's e-discovery process were many months of delay in imposing a litigation hold and in advising the vendor in charge of managing its information technology systems of the hold as well as orders to permanently delete ESI in the form of emails and email folders of two key figures in the company, including one of the defendants.[81] In addition to granting the defendants' request for an adverse inference jury instruction, Judge Scheindlin awarded them reasonable costs, including attorney's fees, that were associated with bringing their motion.[82]

Even the Internal Revenue Service is facing the consequences from questionable document retention policies and the failure to stop destruction processes when it seemed likely that there would be an investigation of the handing of applications for tax-exempt status by the director of the

---

[76] Zest IP Holdings, LLC v. Implant Direct Mfg., LLC, No. 10-0541-GPC(WVG), 2013 WL 6159177 (S.D. Cal. Nov. 25, 2013).

[77] Herrmann v. Rain Link, Inc., No. 11-1123-RDR, 2013 WL 4028759 (D. Kan. Aug. 7, 2013).

[78] *Id.* at *3.

[79] 945 F. Supp. 2d 494 (S.D.N.Y. 2013).

[80] *Id.* at 497 (footnotes omitted).

[81] *Id.* at 499–501.

[82] *Id.* at 509–10.

IRS's Exempt Organization Unit. A recent article reported that among the problems were "seven hard drive crashes, the lack of a centralized archive, a practice of erasing and reusing backup tapes every six months, and an IRS policy of allowing employees to decide for themselves which e-mails constitute an official agency record."[83] The article notes that the IRS system had an email limit of 150 megabytes per mailbox (about 1,800 emails), that some employees used a "print and save" approach, and that many times email attachments were not saved at all.[84]

B. Discovery

[Add the following to the section.]

A search of the K&L Gates Electronic Discovery Case Database and the Kroll Ontrack database[85] for cases since June 2013 indicates that discovery of email continues to be a serious matter for clients and their lawyers, resulting in claims of spoliation and lack of cooperation, motions for sanctions, motions to compel, and disputes about the adequacy of search, identification or collection methods and over the format of production, privilege and metadata. These cases concern employment discrimination and/or hostile work environment,[86] breach of contract and trade secret misappropriation,[87] product liability,[88] copyright and trademark infringement and unfair competition,[89] a variety of federal and state laws,[90] patent infringement,[91] and breach of contract and conversion.[92] Additional cases

---

[83]Gregory Korte, *Long List of Reasons Contributed to Lost IRS E-Mails: Agency Failed to Save Crucial Documents*, USA Today for the Indianapolis Star (June 18, 2014), at 3B, *available at* http://www.usatoday.com/story/news/politics/2014/06/17/how-the-irs-lost-lois-lerners-e-mails/10695507/.

[84]*Id.*

[85]K&L Gates, E-Discovery Case Database, http://www.ediscoverylaw.com/e-discovery-case-database/ and http://www.ediscovery.com/pulse/case-law/.

[86]Brown v. West Corp., No. 8:11CV284, 2013 WL 6263632 (D. Neb. Dec. 4, 2013); Hixson v. City of Las Vegas, No. 2:12-cv-00871-RCJ-PAL, 2013 WL 3677203 (D. Nev. July 11, 2013); Knickerbocker v. Corinthian Colls., No C12-1142JLR, 2014 WL 1356205 (W.D. Wash. Apr. 7, 2014).

[87]Hull v. WTI, Inc., 744 S.E.2d 825, 2013 WL 2996191 (Ga. Ct. App. 2013).

[88]*In re* Zoloft (Sertraline Hydrochloride) Prods. Liability Litig., MDL No. 2342, 2013 WL 8445354 (E.D. Pa. Oct. 31, 2013); SJS Distribution Sys., Inc. v. Sam's East, Inc., No. 11 CV 1229(WFK)(RML), 2013 WL 5596010 (E.D.N.Y. Oct. 11, 2013) (claims related to packaging intended for resale).

[89]Sophia & Chloe, Inc. v. Brighton Collectibles, Inc., No. 12cv2472-AJB(KSC), 2013 WL 5212013 (S.D. Cal. Sept. 13, 2013).

[90]Stream Cos., Inc. v. Windward Adver., No. 12-cv-4549, 2013 WL 3761281 (E.D. Pa. July 17, 2013).

[91]Surfcast v. Microsoft Corp., No. 2:12-cv-333-JAW, 2013 WL 4039413 (D. Me. Aug. 7, 2013).

[92]Teledyne Instruments, Inc. v. Cairns, No. 6:12-cv-854-Orl-28TBS, 2013 WL 5781274 (M.D. Fla. Oct. 25, 2013).

concern insurance disputes,[93] lack of specificity in discovery requests,[94] and whether a deposition request about search methodology was unduly burdensome.[95] Interestingly, the discoverability of email messages and their use as documentary evidence are the subjects of two related pieces of legislation introduced in Congress over the past year. First, S.1013, the Patent Abuse Reduction Act of 2013,[96] provides a long list of criteria that qualify as "core documentary evidence." However, this definition excludes "any computer code or electronic communication, such as e-mail, text messages, instant messaging, and other forms of electronic communication, unless the court finds good cause."[97] In what appears to be a more expansive version for purposes of discovery, H.R.3309, the Innovation Act,[98] "[p]rovides for discovery of electronic communications (including emails, text messages, or instant messages) only if the parties determine that it is appropriate under procedures that address whether such discovery is to occur after the parties have exchanged initial disclosures and core documentary evidence."[99]

1. Attorney-Client Privilege

[Add the following at the end of the section.]

Since July 2011, a number of cases have addressed the issue of privilege for email that was requested as part of the discovery process. These cases suggest that courts are becoming more comfortable within the realm of electronic discovery and the responsibilities of clients and counsel for preservation and production of electronically stored information and less patient when the appropriate steps and safeguards are not in place, especially with respect to privilege.

Another theme of some of the cases is the failure of the party or its counsel to address inadvertent disclosure in a timely manner. For example, in *Ceglia v. Zuckerberg*[100] the court held that the attorney-client privilege

---

[93] Shaw Group Inc. v. Zurich Am. Ins. Co., No. 12-257-JJB-RLB, 2014 WL 1891543 (M.D. La. May 12, 2014).

[94] American Home Assurance Co. v. Greater Omaha Packing Co., No. 8:11CV270, 2013 WL 4875997 (D. Neb. Sept. 11, 2013).

[95] Koninklijke Philips N.V. v. Hunt Control Sys., Inc., No. 11-3684 DMC, 2014 WL 1494517 (D.N.J. Apr. 16, 2014).

[96] *See* Summary: S.1013—113th Congress (2013-2014), *available at* https://www.congress.gov/bill/113th-congress/senate-bill/1013.

[97] *Id.*

[98] *See* Summary: H.R.3309—113th Congress (2013-2014), *available at* https://www.congress.gov/bill/113th-congress/house-bill/3309.

[99] *Id. See also* Octane Fitness, LLC v. Icon Health & Fitness, Inc., 134 S. Ct. 1749, 1755, 188 L. Ed. 2d 816, 824, 110 USPQ2d 1337 (2014) (district court had found "no subjective bad faith on ICON's part, dismissing as insufficient both 'the fact that [ICON] is a bigger company which never commercialized the '710 patent' and an e-mail exchange between two ICON sales executives, which Octane had offered as evidence that ICON had brought the infringement action 'as a matter of commercial strategy.'").

[100] No. 10-CV-00569A(F), 2012 WL 1392965, 2012 U.S. Dist. LEXIS 55367 (W.D.N.Y. Apr. 19, 2012).

was waived when an email was inadvertently produced by an information technology expert. The court found that the plaintiff and counsel did not take reasonable steps to prevent disclosure of the email nor did they act promptly to address this lapse once it was discovered, waiting nearly two months after the material was disseminated to request that it be returned or destroyed.[101] In *Williams v. District of Columbia*,[102] the court denied the defendant's motion to exclude an inadvertently produced email because the defendant failed to satisfy the burden of establishing that reasonable steps were taken to prevent disclosure and did not promptly take steps to rectify the error.[103]

Courts are also finding that privilege has been waived when parties do not take reasonable steps to preserve confidentiality. For example, in *Pacific Coast Steel, Inc. v. Leany*,[104] the plaintiff had purchased the assets of several companies in which the defendant had an ownership interest and became a high-level employee. He was later terminated and his computer was seized. PCS claimed that Leany had been previously informed that the computer was the property of PCS, that all documents would be merged into a single PCS server, and that PCS reserved the right to monitor the use of the computer system. Nevertheless, he made no effort to remove any confidential or privileged information during an email migration or upon being terminated. In particular, the court noted that Leany could not have had any expectation of privacy in the emails.[105] This case points to the dangers of waiving privilege for otherwise confidential information when using an employer-provided computer to communicate with accountants, spouses, or attorneys if the employer has reserved the right to monitor usage and has an Acceptable Use Policy for email and other electronic communications systems.

The ABA's Formal Opinion 11-459, August 4, 2011, Duty to Protect the Confidentiality of E-Mail Communications with One's Client, addresses

---

[101] *Id. See* Electronic Discovery Law, Expert's Inadvertent Production Results in Waiver of Privilege Absent Sufficient Supervision by Counsel or Prompt Steps to Rectify Disclosure, *available at* http://www.ediscoverylaw.com/2012/05/articles/case-summaries/experts-inadvertent-production-results-in-waiver-of-privilege-absent-sufficient-supervision-by-counsel-or-prompt-steps-to-rectify-disclosure/ (K&L Gates May 24, 2012) (last visited June 28, 2012).

[102] 806 F. Supp. 2d 44 (D.D.C. 2011). *See* Electronic Discovery Law, Court Denies Motion to Exclude Inadvertently Produced Email, Rejects Argument that 26(b)(5)(B) Request for the Email's Return Satisfied FRE 502(b)(3) Obligation, *available at* http://www.ediscoverylaw.com/2011/09/articles/case-summaries/court-denies-motion-to-exclude-inadvertently-produced-email-rejects-argument-that-26b5b-request-for-the-emails-return-satisfied-fre-502b3-obligation/print.html (K&L Gates Sept. 5, 2011) (last visited June 28, 2012).

[103] *See* Court Denies Motion to Exclude Inadvertently Produced Email, Rejects Argument that 26(b)(5)(B) Request for the Email's Return Satisfied FRE 502(b)(3) Obligation, http://www.ediscoverylaw.com/2011/09/articles/case-summaries/court-denies-motion-to-exclude-inadvertently-produced-email-rejects-argument-that-26b5b-request-for-the-emails-return-satisfied-fre-502b3-obligation/print.html (last visited June 28, 2012).

[104] No. 2:09-cv-12190, 2011 WL 4573243, 2011 U.S. Dist. LEXIS 113849 (D. Nev. Sept. 30, 2011).

[105] *Id.* at *7–8, *11, 2011 U.S. Dist. LEXIS 113849, at *24.

the danger of third-party access to client communications.[106] The opinion discusses two common examples of how the attorney-client privilege can be put at risk: employer-provided email, where the employer has indicated that it has the right to monitor emails (and the party communicates with counsel via the email account), and where a family member can access an email account (and the party is involved in a matrimonial dispute). The opinion, which echoes a number of recent cases, suggests the need to educate the client about this risk and obtain consent to how he/she would like to be communicated with.

An article by Stagg and Anderson[107] highlights this issue in the context of attorney-client privilege in Tennessee, first reviewing cases from New York, New Jersey, and California as well as the ABA's Formal Opinion 11-459, and then describing the decision in a recent Tennessee trial court case, *Forrest v. Lewis*.[108] The court in *Forrest v. Lewis* held that the plaintiff had "'no reasonable expectation that his communications to his attorney using company email were private'" and that the emails conveyed through a company email system did not fall within the attorney-client privilege.[109]

A quick search of the K&L Gates database[110] of electronic discovery cases related to email in 2012 illuminates a number of common themes, including: spoliation and sanctions;[111] privilege and waiver;[112] forensic examination of email accounts;[113] cost shifting for processing email accounts;[114] and motions for a protective order over email records, emails, text messages, and other related information from Yahoo! and Verizon.[115]

There have been predictions that use of email would by now be passé and would be bypassed in favor of texting, tweeting, and social media, at least within popular culture. However, from these cases it is clear that email continues to be a major means of communication within the

---

[106]ABA Standing Comm. on Ethics & Prof'l Responsibility, Formal Opinion 11-459, *Duty to Protect the Confidentiality of E-Mail Communications with One's Client* (Aug. 4, 2011), *available at* http://learn.uvm.edu/ce/wp-content/uploads/ABA_Formal_Opinion.pdf (last visited June 28, 2012).

[107]M. Kimberly Stagg & John E. Anderson, Sr., *Cover Story: We Know You've Got Mail*, 49 Tenn. B.J. 12 (Dec. 2013).

[108]No. 15402, 2012 WL 7655289 (Tenn. Ch. Cheatham County Dec. 4, 2012) (Trial Order).

[109]Stagg & Anderson, *Cover Story* at 15 (quoting *Forrest*, 2012 WL 7655289, at *3).

[110]E-Discovery Case Database, K&L Gates, http://www.ediscoverylaw.com/articles/ediscovery-case-database/ (last visited Sept. 11, 2012).

[111]Danny Lynn Elec. v. Veolia Es Solid Waste, No. 2:09CV192, 2012 WL 786843, 2012 U.S. Dist. LEXIS 31685 (M.D. Ala. Mar. 9, 2012); Hudson v. AIH Receivable Mgmt. Servs., No. 10-2287, 2012 WL 1194329, 2012 U.S. Dist. LEXIS 49189 (D. Kan. Mar. 14, 2012).

[112]Goldstein v. Colborne Acquisition Co., No. 10 C 6861, 2012 WL 1969369, 2012 U.S. Dist. LEXIS 75743 (N.D. Ill. June 1, 2012); Jacob v. Duane Reade, Inc., No. 11 Civ. 0160, 2012 WL 651536, 2012 U.S. Dist. LEXIS 25689 (S.D.N.Y. Feb. 28, 2012).

[113]Moore v. Kingsbrook Jewish Med. Ctr., Nos. 11-CV-3552, 11-CV-3624, 2012 WL 1078000, 2012 U.S. Dist. LEXIS 45738 (E.D.N.Y. Mar. 30, 2012).

[114]Rawal v. United Air Lines, Inc., No. 07 C 5561, 2012 WL 581146, 2012 U.S. Dist. LEXIS 21880 (N.D. Ill. Feb. 22, 2012).

[115]Special Mkts. Ins. Consultants, Inc. v. Lynch, No. 11 C 9181, 2012 WL 1565348, 2012 U.S. Dist. LEXIS 61088 (N.D. Ill. May 2, 2012).

business community, so it still should be a matter of concern in the context of electronic discovery, as well as for overall information management.

Care needs to be taken throughout the electronic discovery process when handling email as electronically stored information (ESI). Given the sheer volume of email that might be generated by even a small company or individual client, inadvertent production may pose a special risk because courts may deem that this results in a waiver of the attorney-client privilege. For example, in *Inhalation Plastics, Inc. v. Medex Cardio-Pulmonary, Inc.*,[116] the court held that privilege had been waived for 347 pages of email which had been inadvertently produced, out of a batch of 7500 pages that had been produced as hard copy without marking anything as confidential, finding that the defendant had failed to establish that it had taken reasonable precautions to prevent the disclosure and then failed to take adequate measures to rectify or mitigate the damage from the disclosure.[117] In its analysis of whether privilege had been waived, the court discussed the three-factor analysis from Federal Rule of Evidence 502(b) and a five-factor test that is generally used to determine whether a party's documents should be returned.[118] The court was also persuaded by the sheer number of documents that were inadvertently disclosed (4.6 percent), the lack of a privilege log at the time of the disclosure, the relevance of the documents to the dispute, and whether several layers of attorneys had participated in the review.[119]

One facet of the attorney-client privilege that is receiving attention in 2013 is how the attorney-client privilege is applied to in-house counsel. In *United States ex rel. Baklid-Kunz v. Halifax Hospital Medical Center*,[120] a federal magistrate judge took a rather narrow approach in applying a rule that communications between a client and a corporate attorney about business matters or business advice are not privileged unless they "solicit or predominantly deliver legal advice." In so doing, he held that hundreds of documents and communications, including audit and review materials and emails that were sent between the finance and legal department involving Halifax Hospital's inside counsel, were not privileged and granted the privilege narrowly only to documents that sought or reflected legal advice. First, the judge provided an analysis of assertions of privilege over email communications in the corporate setting and adopted the rule that each email in an email string must be listed separately on a privilege log.[121] Then the judge addressed each of the seven categories where

---

[116] No. 2:07-CV-116, 2012 WL 3731483 (S.D. Ohio Aug. 28, 2012). *See* Inadvertent Production Results in Waiver of Attorney-Client Privilege as to 347 Pages of Emails, *available at* http://www.ediscoverylaw.com/2012/09/articles/case-summaries/inadvertent-production-results-in-waiver-of-attorneyclient-privilege-as-to-347-pages-of-emails/ (K&L Gates, September 12, 2012) (last visited June 21, 2013).

[117] *Id.*

[118] *Id.*

[119] *Id.*

[120] No. 6:09-cv-1002-Orl-31TBS, 2012 U.S. Dist. LEXIS 158944 (M.D. Fla. Nov. 6, 2012).

[121] *Id.* at *11–15.

a determination of privilege was requested.[122] The opinion includes detailed charts of his rulings with respect to specific documents, such as Category 3 related to documents or communications that relate to internal audits and reviews[123] and Category 6 covering email strings.[124] Interestingly, a significant majority of the rulings listed on the charts indicate that the material was deemed not privileged, often because either no legal advice was sought or received or because of no attorney "to" or "from."

In a short article analyzing this case, Kim notes that "[t]he Halifax decision reflects the growing scrutiny that courts are applying to businesses asserting attorney-client privilege over documents involving in-house counsel."[125] The author notes that although this is not a new issue, the increased scrutiny can be attributed to the expanded role of in-house counsel in providing business advice as well as legal advice, due to their experience in the commercial setting, and that courts have been inconsistent in how they have evaluated attorney-client privilege claims.[126] She concludes that:

> Courts have recognized certain practices—such as addressing the in-house attorney in the "to" line as opposed to the "cc" line in emails, structuring important compliance audits to be conducted under the direction of in-house attorneys, and limiting the number of people included in a communication—to trigger attorney-client privilege. To gain more certainty in retaining confidentiality in documents and communications, in-house counsel for healthcare institutions will need to be more explicit and deliberate in applying these recognized practices in the future to ensure that institutional documents and communications remain protected under the attorney-client privilege.[127]

An article by Judish and Assay provides additional insight into the case and also includes a list of best practices for communications with general counsel, with the observation that this case and others discussed in their article serve as "important cautions to organizations that assume the inclusion of general counsel in discussions automatically confers privilege on such discussions."[128]

There is often an assumption, especially among clients, that including in-house lawyers as recipients of a communication or copying them in email circulation will mean that the document is protected by privilege. Desoer, Lambert, and Wites provide a thoughtful analysis of this

---

[122] *Id.* at *17–37.

[123] *Id.* at *25–27.

[124] *Id.* at *21–24.

[125] Judith Kim, *Attorney-Client Privileged Documents: Federal District Court Limits the Scope of Attorney-Client Privilege Granted Involving In-House Counsel*, 39 Am. J. L. and Med. 186, 187 (2013).

[126] *Id.*

[127] *Id.* at 188.

[128] Julia E. Judish & Stephen S. Asay, *Federal Court Sets Guidelines Denying Attorney-Client Privilege on Communications*, *available at* http://www.pillsburylaw.com/publications/federal-court-sets-guidelines-for-denying-attorney-client-privilege (Pillsbury Mar. 11, 2013) (last visited June 21, 2013).

situation, emphasizing that the determination of whether the privilege has been asserted properly may require more detailed information.[129]

An article by DeLisi addresses the issue of protecting attorney-client privilege in an era where many, if not most, employers have Acceptable Use policies governing email, Internet, social media and other technology and which include the right to monitor employee communications through this technology.[130] He advocates a three-pronged approach:

> First, lawyers should seek to prevent nonconfidential communications from occurring by discussing the degree of confidentiality of their client's workplace systems and how the lack of confidentiality might undermine attorney-client privilege. Second, if employers monitor attorney-client communications, employers should attempt to avoid reading them so that, even though they were technically nonconfidential, courts may still consider them privileged. Third, courts should allow the privilege to attach when the employee believed that her communications with her attorney were confidential.[131]

A recent article by Favro provides an excellent discussion of the impact of new technologies on the attorney-client privilege for in-house counsel and includes some suggested practices to enhance the defensibility of in-house counsel's privilege claims.[132]

Recent ethics opinions address the risks associated with communicating by email. One of the issues is whether lawyers should respond to emails with the "Reply All" option.[133] Another issue focuses on confidential written communications between the opposing party and his or her counsel are sent by a nonparty, but where the receiving lawyer believes that the circumstances may suggest that the crime-fraud exception applies to the attorney-client privilege.[134]

---

[129] Michele Desoer, Lawrence B. Lambert & Marc A. Wites, *Does Copying an In-House Lawyer on Corporate Correspondence Render It Privileged?*, The Federal Lawyer (Mar. 2014), at 60–63, 70.

[130] Alex DeLisi, *Note: Employer Monitoring of Employee Email: Attorney-Client Privilege Should Attach to Communications That the Client Believed Were Confidential*, 81 Fordham L. Rev. 3521 (May 2013).

[131] *Id.* at 3524.

[132] Philip J. Favro, *Inviting Scrutiny: How Technologies Are Eroding the Attorney-Client Privilege* (Apr. 13, 2013). SSRN, http://ssrn.com/abstract=2255206 (last visited June 24, 2013).

[133] Karen A. Gledhill, *State Bar Adopts Ethics Opinion Impacting Email Communications*, Notes Bearing Interest (Newsletter of the Business Law Section of the N.C. Bar Association, Nov. 1, 2013), Robinson Bradshaw, *available at* http://www.rbh.com/state-bar-adopts-ethics-opinion-impacting-email-communications-11-01-2013/ (last visited June 19, 2014).

[134] The State Bar of California, Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2013-188, *available at* http://ethics.calbar.ca.gov/Portals/9/documents/Opinions/CAL%202013-188%20%2806-0004%29.pdf (last visited June 19, 2014).

An article on email etiquette also covers important issues with respect to maintaining the confidentiality of client information.[135] The author's recommendations for email correspondence that intersect with client confidentiality and attorney-client privilege include whether email should be sent at all because of the potential for it being discoverable; confining an email message to a single or related group or subjects; clarifying the status of drafts and revisions sent via email; writing with the presumption that the client will forward the email even if warned not to; security concerns with wireless devices, unsecure networks, hacking and eavesdropping; guarding against emotional outbursts in email; verifying receipt; and checking email attachments before sending.[136]

2. Possession/Custody/Control

[Add the following at the end of the section.]

In 2012, the American Bar Association Commission on Ethics 20/20 circulated drafts of amendments to rules and comments that reflect the modern realities of the practice of law, particularly issues that relate to the increasing use of technology to manage law firms and to deliver legal services more efficiently and economically. A number of materials were filed with the ABA House of Delegates on May 7, 2012, for consideration at the ABA's annual meeting in Chicago in August 2012. Among the filings were resolutions and reports on technology and confidentiality, technology and client development, and outsourcing that could encompass email and other electronic means of communication within law firms, with clients, and with third parties and which may depend on the services of third-party and Cloud computing vendors.[137]

On August 6, 2012, the ABA's House of Delegates voted to approve changes to the ABA Model Rules of Professional Conduct "to provide guidance regarding lawyers' use of technology and confidentiality as follows.…"[138] Resolution 105A makes several changes regarding email:

- Model Rule 1.0 Terminology: In Section (n), "e-mail" is amended to "electronic communications";
- Model Rule 1.0, Comment [9] (Screened): Screening includes avoiding contact with or denying access to "information, including information in electronic form," which relates to the matter;

---

[135] George W. Kuney, *Legal Form, Style, and Etiquette for Email*, 15 Transactions 59 (Fall 2013).

[136] *Id.*

[137] *See* ABA Commission on Ethics 20/20, *available at* http://www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html (last visited June 28, 2012).

[138] Resolution 105A Revised, http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf (last visited Sept. 11, 2012).

- Model Rule 1.1 Competence, Comment [6] (Maintaining Competence): Rule 1.1's admonition that a lawyer should maintain "requisite knowledge and skill" by keeping "abreast of changes in the law and its practice" now includes in such practice "the benefits and risks associated with relevant technology";
- Model Rule 1.6 Confidentiality of Information: Section (c) is added whereby "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." The expectations are illuminated in the amendments to Comment [16] (Acting Competently to Preserve Confidentiality);
- Model Rule 4.4 Respect for Rights of Third Persons: Section (b) now adds "electronically stored information" as material whose inadvertent receipt requires a prompt notification to the sender;
- Model Rule 4.4, Comment [2] describes how a document or electronically stored information is inadvertently sent when it is accidently transmitted, for example, as when an email or letter is misaddressed.[139]

Lawyers are urged to review these proposed revisions to the Rules as well as to read the report that accompanies these revisions to fully understand what their ethical responsibilities may be, given that many, if not most, states are likely to adopt the same or similar revisions. In addition, lawyers will want to review the revisions in Resolution 105B dealing with technology and client development to see the extent to which it impacts advertising and solicitation using email or other electronic means as well as the multijurisdictional practice of law.[140]

The impact of the Stored Communications Act and whether this protects electronically stored information has been a continuing theme in the development of electronic discovery processes. In *Optiver Australia Pty. Ltd. & Anor v. Tibra Trading Pty. Ltd. & Ors*,[141] the court addressed what qualifies as "content" so that disclosure by service providers would be prohibited under the SCA.[142] The plaintiff had issued a subpoena to Google requesting emails, email attachments and Google Talk messages sent by the employee's defendants, including metadata related to messages containing certain search terms and the subject lines of those messages

---

[139] *Id.*

[140] Resolution 105B, *available at* http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105b.authcheckdam.pdf (last visited June 28, 2012).

[141] No. C 12-80242 EJD (PSG), 2013 WL 256771 (N.D. Cal. Jan. 23, 2013).

[142] *See* Court Considers the "Persnickety, but Persistent Question" of What Qualifies as "Content" Under the Stored Communications Act (K&L Gates Feb. 20, 2013), *available at* http://www.ediscoverylaw.com/2013/02/articles/case-summaries/court-considers-the-persnickety-but-persistent-question-of-what-qualifies-as-content-under-the-stored-communications-act/ (last visited June 24, 2013)).

and others which met criteria, such as time frame or recipients.[143] Most of this information was deemed to be "content" protected under the SLA. As stated by the court,

> [t]he SCA prohibits *any* knowing disclosure by service providers of the content of electronic communications, no matter how insignificant. The search proposed by Optiver would necessarily reveal that the emails identified contain the terms "PGP" or "Optiver," which are words contained in the body of the communications. These terms constitute content, or information concerning the "substance, purport, or meaning" of the communications. However trivial, this is exactly the sort of information the SCA sought to protect.[144]

The court did allow the plaintiff to receive non-content metadata.[145] On the other hand, in *Garcia v. City of Laredo*,[146] the Fifth Circuit affirmed the district court's interpretation of the Stored Communications Act, concluding that it does not apply to data stored on a personal cell phone because a cell phone is not an SCA-protected "facility."[147]

The interpretation of the Stored Communications Act and whether it protects electronically stored information (ESI) continues to evolve in electronic discovery case law. For example, in *Cheng v. Romo*,[148] the court was asked to determine whether Web-based emails are "electronic storage" as defined by the Stored Communications Act. After discussing case law and commentary identifying imperfections in the Act's statutory language and reviewing the definition of "electronic storage" found at 18 U.S.C. §2510(17)(B), the court found that the SCA did apply because the Web-based server continued to store copies of the emails that had been transmitted to both the plaintiff's and the defendant's Web browsers.[149]

C. Cross-Border Issues

[Add the following at the end of the section.]

Outsourcing of many of the functions of a law firm may raise cross-border issues with respect to email and other electronic communications. As part of its work, the ABA Commission on Ethics 20/20 recently

---

[143] *Optiver Australia*, 2013 WL 256771, at *1.

[144] *Id.* at *2 (emphasis added).

[145] *Id.* at *3.

[146] No. 11-41118, 2012 WL 6176479 (5th Cir. Dec. 12, 2012).

[147] *See* Fifth Circuit: "We conclude that the Stored Communications Act … does not apply to data stored in a personal cell phone," *available at* http://www.ediscoverylaw.com/2013/01/articles/case-summaries/fifth-circuit-we-conclude-that-the-stored-communications-act-does-not-apply-to-data-stored-in-a-personal-cell-phone/ (K&L Gates Jan. 21, 2013) (last visited June 21, 2013)).

[148] No. 11-10007-DJC, 2013 WL 6814691 (D. Mass. Dec. 20, 2013).

[149] *Id.*; *see also* Opened, Web-based Emails Are "Electronic Storage" as Defined by the Stored Communications Act, ediscovery.com, *available at* http://www.ediscovery.com/pulse/case-law/detail/26541/#.VFjAQ8t0ypp (Kroll Ontrack) (last visited June 18, 2014).

released its resolution and report dealing with outsourcing.[150] Among the revisions approved by the ABA House of Delegates in August 2012 are the following changes:

- Model Rule 1.1 Competence, Comments [6] & [7] (Retaining or Contracting With Other Lawyers): These two new Comments illuminate the ethical responsibilities for retaining or contracting with other lawyers. One aspect of this related to cross-border issues is the possibility that these lawyers may be located in other countries, thus necessitating the need to communicate via email and other electronic means which may not necessarily be protected by laws and regulations in those counties, as well as making sure that lawyers in those countries are properly apprised of their responsibilities for handling confidential materials in a secure manner.[151]
- Model Rule 5.3 Responsibilities Regarding Nonlawyer Assistance: In the title, a subtle but significant change is made from "Assistants" to "Assistance." New Comments [3] & [4] address the use of nonlawyers outside the firm and provide as examples the hiring of a document management company to create and maintain a database for complex litigation, sending client documents to a third party for printing or scanning, and using an Internet-based service to store client information. Comment [3] makes it clear the lawyer must make reasonable efforts to make sure that services that are outsourced to nonlawyers are provided in a manner that is compatible with the lawyer's professional obligations. This Comment also references several of the other rules, including Rule 1.1 Competence, Rule 1.6 Confidentiality, and Rule 5.5(a) Authorized Practice Of Law.

Cross-border issues with respect to email are already receiving considerable attention due to the recent disclosures about NSA surveillance. One bill, H.R. 2399, the Limiting Internet and Blanket Electronic Review of Telecommunications and Email Act, or LIBERT-E Act, was introduced on June 17, 2013.[152] The bill addresses and attempts to limit and provide oversight for surveillance of many types of electronic communication, including email.

As more information is released about the scope of the activities of Edward Snowden, the extent of the NSA's surveillance programs is being revealed. Among the surveillance systems in place are not only those that collect information about email activity, including both domestic and

---

[150] Resolution 105C, *available at* http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105c.authcheckdam.pdf (last visited June 28, 2012).

[151] Former Comment [6] is redesignated as Comment [8] (Maintaining Competence).

[152] *See* Summary: H.R.2399—113th Congress (2013-2014), *available at* https://www.congress.gov/bill/113th-congress/house-bill/2399.

cross-border email, but also those systems that can search the content of email messages.[153] Out of concern for the protection of client confidentiality and the duties of lawyers under Model Rules 1.1 and 1.6, especially as it relates to the appropriate use of technology for rendering legal services, the American Bar Association issued its Resolution 118 on cybersecurity at its House of Delegates Meeting in August 2013.[154] The resolution states that the American Bar Association "condemns unauthorized, illegal governmental, organizational and individual intrusions into the computer systems and networks utilized by lawyers and law firms" and also "opposes governmental measures that would have the effect of eroding the attorney-client privilege, the work product doctrine, the confidential lawyer-client relationship, or traditional state court and bar regulation and oversight of lawyers and the legal profession."[155] The resolution also encourages lawyers and law firms to

> review and comply with the provisions relating to the safeguarding of confidential client information and keeping clients reasonably informed that are set forth in the Model Rules of Professional Conduct, as amended in August 2012 and as adopted in the jurisdictions applicable to their practice, and also comply with other applicable state and federal laws and court rules relating to data privacy and cybersecurity.[156]

Nelson and Simek continue to provide practical and timely information about the security risks to law firms. A short article published in January 2014 raised questions about the NSA's XKeyscore program, noting that the program allows NSA to gather phone numbers, email addresses, and metadata as well as see email content, browser history, and an IP address without obtaining a warrant and that this information can be stored for later analysis.[157] The authors state that "while the NSA's purported mission is to target foreigners, the NSA sometimes retains the written content of e-mails sent between citizens with [*sic*] the U.S."[158] The authors

---

[153] John Biggs, *NSA Project XKeyscore Collects Nearly Everything You Do on the Internet*, TechCrunch (Jul. 31, 2013), *available at* http://techcrunch.com/2013/07/31/nsa-project-x-keyscore-collects-nearly-everything-you-do-on-the-Internet/ (last visited June 18, 2014); Alex Wilhelm, *The NSA Searches US Citizens' Cross-Border Email That Mentions Foreign Targets*, TechCrunch (Aug. 8, 2014), *available at* http://techcrunch.com/2013/08/08/nytimes-the-nsa-searches-us-citizens-cross-border-email-that-mentions-foreign-targets/ (last visited June 18, 2014); Chris Strohm, *NSA Searched E-Mail, Phone Calls of Americans: Clapper*, Bloomberg (Apr. 1, 2014), http://www.bloomberg.com/news/2014-04-01/nsa-searched-e-mail-phone-calls-of-americans-clapper.html (last visited June 18, 2014).

[154] ABA Resolution 118 (Aug. 2013), *available at* http://www.americanbar.org/content/dam/aba/administrative/law_national_security/resolution_118.authcheckdam.pdf (last visited June 18, 2014).

[155] *Id.* at 1.

[156] *Id.*

[157] Sharon D. Nelson & John W. Simek, *What NSA Surveillance Means to Law Firms* (Sensei Enterprises 2014), *available at* https://static.squarespace.com/static/5006ee71e4b0830a a852a93f/52edad99e4b04a6158a3796e/52edad9be4b04a6158a37ff8/1389300882227/What%20NSA%20Surveillance%20Means%20to%20Law%20Firms%20-%202014A.pdf (last visited June 18, 2014).

[158] *Id.* at 3.

offer advice related to law firm use of cloud computing, of encryption, of allowing BYOD only with a Mobile Device Management (MDM) solution implemented, of moving data out of the U.S. in favor of having it stored in the United States with companies that pledge not to cooperate with the government, of passwords, of security audits, and of training.[159] Our preference is to use encryption and recommend that lawyers consult an article by Holahan and Hussain on the basics of encryption.[160]

A more expansive article by Nelson and Simek[161] from March 2014 discusses Edward Snowden's revelations about the NSA's activities, including access to the Google and Yahoo! accounts of Americans, the XKeyscore program, harvesting of emails and instant messaging contact lists, searching email content, tracking and mapping the location of cell phones, and tapping into Google and Yahoo! data centers. The article raises specific concerns for lawyers about how they communicate and access information using email and other technologies. It relates a story from the *New York Times* from February 2014 wherein a

> top-secret document demonstrated that an American law firm was monitored while representing a foreign government in trade disputes with the United States. The government of Indonesia had retained the law firm for help in trade talks, according to the February 2013 document. It reports that the NSA's Australian counterpart, the Australian Signals Directorate, notified the NSA that it was conducting surveillance of the talks, including communications between Indonesian officials and the American law firm, and offered to share the information.[162]

Nelson and Simek report that ABA President James R. Silkenat asked the NSA's Director for an explanation of what policies and practices the NSA has in place to protect confidential attorney-client privilege that may be received or intercepted as well as whether these policies and practices were followed in the alleged law firm incident.[163] The authors relate that while there is considerable discussion about keeping sensitive information out of email messages, telephone conversations, and video conferencing systems, this also supports the need for using encryption to protect confidential client data and communications.[164] They suggest that perhaps that distrust of state-sponsored surveillance may result in a return to the past practice of face-to-face communications that are free from cameras or audio surveillance systems.[165]

---

[159] *Id.* at 3–5.

[160] Shawn L. Holahan & Abid Hussain, *Solo Speaking: Encryption: The Basics*, 61 La. B.J. 121 (Aug./Sept. 2013).

[161] Sharon D. Nelson & John W. Simek, *Edward Snowden: How Will NSA Revelations Change the Profession of Law?* (Sensei Enterprises 2014), *available at* http://static.squarespace.com/static/5006ee71e4b0830aa852a93f/t/531dc2a7e4b091b37777586a/1394459303914/Edward%20Snowden.pdf (last visited June 18, 2014).

[162] *Id.* at 5.

[163] *Id.* at 6.

[164] *Id.* at 8.

[165] *Id.*

III. Issues Arising Out of Impermissible Use of Email

A. Spam

2. The CAN-SPAM Act

a. What Is Covered

ii. "Transactional or Relationship Content"

[Add the following at the end of the section.]

At least one court has held that "opting in" (*i.e.*, providing consent to receive emails) does *not* constitute a prior relationship or transaction such that it would take those emails to which consent was given outside the definition of "commercial electronic mail" message.[166]

iii. "Hybrid" Messages

[93][Replace the *MySpace* citation in footnote 93 with the following.] 2007 WL 1686966 (C.D. Cal. 2007).

v. "Initiating Transmission"

[Add the following at the end of the section.]

The question of what constitutes "initiat[ing] the transmission" of covered emails arose recently in the context of social media messaging in *Facebook, Inc. v. Power Ventures, Inc.*[167] Defendant Power Ventures, Inc. offered users the ability to access multiple social networking accounts through a single, integrated Web site at www.power.com. As a promotion of its Web site, Power offered users the chance to win $100 if they successfully invited and signed up new Power.com users. Power used participants' Facebook login credentials to obtain a list of their Facebook friends, and asked the participants to select which of those friends should receive an invitation to a Facebook "event" promoting Power's Web site. Those invitations purported to come from "Facebook" and used an "@facebookmail.com" address, not a Power.com address.[168]

In cross-motions for summary judgment, the parties disputed whether Power "initiated" the emails at issue or whether, as Power argued, Power could not have initiated the emails because the emails were authorized

---

[166]United States v. Rad, 559 Fed. App'x 148 (3d Cir. 2014).

[167]No. C 08-05780, 2012 WL 542586, 2012 U.S. Dist. LEXIS 25062 (N.D. Cal. Feb. 16, 2012), *motion for reconsideration denied*, No. 08-CV-5780-LHK, 2013 WL 5372341 (N.D. Cal. Sept. 25, 2013).

[168]*Id.* at *1, 2012 U.S. Dist. LEXIS 25062, at *5.

by Facebook users and sent from Facebook's own servers. It was undisputed that:

(1) Power.com authored the text contained in the emails and provided the link contained therein that would allow recipients to sign up for Power.com;

(2) the launch promotion feature that offered the $100 reward was made available through Power.com (not through any social network);

(3) Power created and used a script that would automatically send event invitations to a user's Facebook friends;

(4) Power paid 30 to 40 people who got 100 or more friends to sign up; and

(5) Power.com's "offer of potential monetary compensation may have induced some Facebook users to participate in Power's launch program."[169]

The court found Power "originated" the emails by intentionally causing Facebook's servers to send emails written by Power, through the use of a software program Power specifically created to cause Facebook's servers to send those emails.[170] To the extent that Facebook users authorized any of these actions, the court found that Power procured that authorization by "offering and awarding monetary incentives."[171]

b. Requirements of CAN-SPAM Act

i. Requirements for All Categories of Email

b) No False Header Information

[Add the following to the bulleted list at the end of the section.]

- It contains a generic or nonsensical "from" name and is sent from a privacy-protected domain name, such that the recipient cannot identify the sender from the "from" name or the publicly available WHOIS information.[172]
- The domain name from which the email was sent was obtained from a registrar who prohibits "spam" practices, and the sender registered the domain with the intent to engage in prohibited practices.[173]

---

[169] *Id.* at *6, 2012 U.S. Dist. LEXIS 25062, at *20–21.

[170] *Id.* at *7, 2012 U.S. Dist. LEXIS 25062, at *22.

[171] *Id.*, 2012 U.S. Dist. LEXIS 25062, at *22–23.

[172] ZooBuh, Inc. v. Better Broadcasting, LLC, No. 2:11cv00516, 2013 WL 2407669, at *6 (D. Utah May 31, 2013).

[173] *Id.*

ii. Requirements for "Commercial" Email

[Add the following at the end of the section.]

In *ZooBuh, Inc. v. Better Broadcasting, LLC*,[174] the U.S. District Court for the District of Utah held that the disclosures required by 15 U.S.C. §7704(a)(5) are not "clear and conspicuous" if they are provided in the email through a remotely hosted image. The court found that many email clients can be configured to view emails as plain text, and cited a variety of government and industry sources recommending that users disable HTML and/or the downloading of remote images to guard against security threats. The court further observed that remotely-hosted images typically are not maintained on the hosting server for a very long time; once the image is removed from the server, the image can never be viewed by the recipient. Accordingly, the court found that information contained in remotely-hosted images "is not likely to appear on the recipient's screen for a duration and in a location sufficiently noticeable for an ordinary consumer to read and comprehend it."[175]

iv. Enforcement

d) Backlash: Opportunistic Plaintiffs

[160][Add the following at the end of footnote 160.] *See* ZooBuh, Inc. v. Better Broadcasting, LLC, No. 2:11cv00516, 2013 WL 2407669 (D. Utah May 31, 2013) (finding plaintiff was "bona fide" Internet access service provider in part because it had "sole ownership of all the hardware, complete and uninhibited access to the hardware, and sole physical control over the hardware" through which it hosted and provided Internet access service to its 35,000 customers around the world; and using Facebook v. Power Ventures, Inc., 844 F. Supp. 2d 1025 (N.D. Cal. 2012), in which the court found that 60,000 messages constituted an adverse effect on a network of 901 million users maintained by over 3,000 employees, as a benchmark for determining whether the volume of messages can be characterized as "negligible").

[161][Add the following at the end of footnote 161.] ; Beyond Sys., Inc. v. Kraft Foods, Inc., 972 F. Supp. 2d 748 (D. Md., 2013).

3. State Statutes

[Add the following new section heading at the beginning of the section.]

[174]No. 2:11cv00516, 2013 WL 2407669 (D. Utah May 31, 2013).
[175]*Id.* at *8–9.

a. Preemption [New Heading]

[164][Add the following before the *But see* signal in footnote 164.] ; Wagner v. Spire Vision, No. C 13-04952 WHA, 2014 WL 889483 (N.D. Cal. Mar. 3, 2014).

[170][Add the following at the end of footnote 170.] *Cf.* Moreland v. AD Optimizers, LLC, No. 5:13-CV-00216-PSG, 2013 WL 3815663 (N.D. Cal. July 18, 2013) (claim for violation of California anti-spam act must meet heightened pleading requirements of Federal Rule of Civil Procedure 9(b)).

[Add the following at the end of the section.]

In *Capp v. Nordstrom, Inc.*,[176] the defendant moved to dismiss claims brought under California's Song-Beverly Credit Card Act of 1974 (Credit Card Act),[177] on the basis that an email address is not "personal identification information" as that term is defined in the Credit Card Act. In the alternative, the defendant argued that if an email address is "personal identification information" under California's Credit Card Act, then the Credit Card Act is preempted by the CAN-SPAM Act.

Looking to the plain language of the CAN-SPAM Act's preemption clause,[178] the court rejected this argument. First, the court held that the CAN-SPAM Act only preempts state statutes that regulate "the manner in which an email is actually transmitted and delivered ('use'), and the content of that email ('commercial messages')," whereas the Credit Card Act "only regulates the *request for* the email address." Second, the court held that the CAN-SPAM Act preempts a statute only if it "specifically and unequivocally applies to email *messages*, and the Credit Card Act only applies to email *addresses*."[179]

[Add the following new section.]

b. Alternative Causes of Action [New Topic]

In the absence of state laws that expressly regulate the use of commercial email, plaintiffs occasionally seek to find other ways to seek relief in state courts. For example, a company called Spam Arrest recently sought over $1 million in damages for 600 allegedly unsolicited emails, asserting, *inter alia*, claims for breach of contract.[180]

---

[176]No. 2:13-cv-00660-MCE-AC , 2013 WL 5739102 (E.D. Cal. Oct. 22, 2013).

[177]Cal. Civ. Code §1747 *et seq.*

[178]15 U.S.C. §7707(b)(1) ("This Act supersedes any statute … of a State … that expressly regulates the use of electronic mail to send commercial messages.…").

[179]*Capp*, 2013 WL 5739102 at *12 (emphasis added).

[180]Spam Arrest, LLC v. Replacements, Ltd., No. C12-481RAJ, 2013 WL 5739102 (W.D. Wash. Aug. 29, 2013).

Spam Arrest offered consumers an "anti-spam" service that worked on a "whitelist" model rather than the more typical "blacklist" one. In other words, rather than attempting to filter out those emails that are most likely unsolicited and commercial in nature, Spam Arrest stopped every email that was not from a "verified" source. Unverified senders were required to complete a "verification process" before their messages could be delivered. Specifically, they were asked to click the "Verify" button on a page of Spam Arrest's Web site. That Web page purported to bind a sender clicking the "Verify" button to Spam Arrest's "Sender Agreement."[181]

Among other things, the Sender Agreement included a representation and warranty that the sender was not violating the CAN-SPAM Act or any other "local, state or federal law governing the transmission of unsolicited commercial email," and provided for liquidated damages of $2,000 for each violation of the Sender Agreement. Spam Arrest claimed that defendant Sentient Jet violated the Sender Agreement 600 times.[182] Cross-motions for summary judgment were filed on the breach of contract claims.

The court granted summary judgment in favor of Sentient Jet, finding that, on the evidence presented by Spam Arrest, no jury could conclude that (1) anyone with authority to bind Sentient Jet entered into the Sender Agreement;[183] or (2) the emails at issue were sent without the recipients' consent (Spam Arrest could not present any of the 600 emails).[184] The court also found Spam Arrest's liquidated damages clause was invalid because $2,000 was not a reasonable forecast of actual damages.[185] The decision in Spam Arrest leaves open the question of whether, if Spam Arrest had been able to produce the emails in question and identify the individuals accepting the Sender Agreement, it could have asserted a successful claim for breach of contract.

---

[181] *Id.* at *2–3.
[182] *Id.* at *4.
[183] *Id.* at *9–10.
[184] *Id.* at *11–13.
[185] *Id.* at *14–18.