Reprinted with Permission
The Bureau of National Affairs, Inc.

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)
KF3095.A77 2011
346.73048--dc23 2011040494

All rights reserved. Photocopying any portion of this publication is strictly prohibited unless express written authorization is first obtained from The Bureau of National Affairs, Inc., 1801 S. Bell St., Arlington, VA 22202, bna.com/bnabooks. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by The Bureau of National Affairs, Inc. for libraries and other users registered with the Copyright Clearance Center (CCC) Transactional Reporting Service, provided that $1.00 per page is paid directly to CCC, 222 Rosewood Dr., Danvers, MA 01923, copyright.com, Telephone: 978-750-8400, Fax: 978-646-8600.

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

Printed in the United States of America
13

Intellectual Property Issues Raised by Email

Michael B. Smith
Sony Computer Entertainment America
Foster City, California

Sara Anne Hook
Indiana University School of Informatics
Indianapolis, Indiana

Aly Dossa
Osha Liang LLP
Houston, Texas

I. Introduction ........................................... 703 —
   A. History of Electronic Messages ................. 703 —
   B. Technical Overview ................................ 703 —
   C. Future of Electronic Communication .......... 704 —
II. Issues Arising Out of Permissible Use of Email ...... 704 155
   A. Privacy/Confidentiality .......................... 704 155
      1. Work vs. Home .................................. 706 156
      2. Document Retention Policies ................. 709 156
   B. Discovery .......................................... 712 157
      1. Attorney-Client Privilege ...................... 712 157
      2. Possession/Custody/Control ................. 717 159
   C. Cross-Border Issues ............................. 720 161
III. Issues Arising Out of Impermissible Use of Email .... 722 162
   A. Spam .............................................. 722 162
      1. Legislative Efforts to Regulate Spam ...... 723 —
2. The CAN-SPAM Act .............................................. 724 162
   a. What Is Covered........................................... 724 162
      i. “Exclusively Commercial” .......................... 724 —
      ii. “Transactional or Relationship
           Content” ............................................. 724 —
      iii. “Hybrid” Messages ................................. 725 162
      iv. “Electronic Mail Messages” ....................... 726 —
      v. “Initiating Transmission” ......................... 727 162
   b. Requirements of CAN-SPAM Act................. 728 —
      i. Requirements for All Categories of
         Email .................................................. 728 —
         a) Headers .......................................... 728 —
         b) No False Header Information ................... 730 —
         c) “Promotion” Liability ............................ 730 —
      ii. Requirements for “Commercial”
          Email ............................................... 731 —
         a) Deceptive Subject Lines ......................... 732 —
         b) Opt-Out Provisions ............................... 732 —
            i) Opt-Out Must be Available for
                at Least 30 Days ............................ 732 —
            ii) No Transmission of
                 Commercial Emails After
                 Opt-out ........................................ 732 —
            iii) No Sharing of Opted-Out
                 Email Address ............................... 733 —
            iv) Subsequent Affirmative
                 Consent ........................................ 733 —
         c) Sending Behavior ................................. 733 —
            i) Address Harvesting and
                Dictionary Attacks ........................... 733 —
            ii) Automatic Creation of Email
                Addresses ...................................... 733 —
                iii) Open Relays/Proxies ...................... 734 —
                iv) Aggravated Violations ..................... 734 —
            iii. Sexually Explicit Email ....................... 734 —
         iv. Enforcement ....................................... 735 —
            a) Federal ......................................... 735 —
            b) State ........................................... 735 —
            c) Private Right of Action ....................... 736 —
            d) Backlash: Opportunistic Plaintiffs ... 737 —
   3. State Statutes........................................... 738 —

B. Phishing..................................................... 740 —
   1. Overview ............................................... 740 —
   2. Technical Overview ................................... 740 —
II. ISSUES ARISING OUT OF PERMISSIBLE USE OF EMAIL

A. Privacy/Confidentiality

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

Two recent pieces of legislation have been introduced in Congress that reflect growing concerns over what should be considered permissible with respect to accessing a person's email. First, HR. 3991, the Keep Employees’ Emails and Phones Secure Act (KEEP Secure Act), which was introduced on February 9, 2012, would amend the National Labor Relations Act to prohibit the National Labor Relations Board (NLRB) from requiring an employer to provide the NLRB or a labor organization with an employee’s telephone number or email address.1 A second bill, H.R. 5050, the Social Networking Online Protection Act, which was introduced

on April 27, 2012, primarily addresses the recent requests by employers to obtain user names and passwords to social media sites such as Facebook from employees or from job applicants as part of the interviewing process.\textsuperscript{2} Note that the language also references attempts to require, request or access private email accounts from employees and job applicants. The bill summary notes that the Act

Prohibits 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 website; 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 \textit{sic} or institutes a proceeding under this Act, or testifies in any such proceeding.\textsuperscript{3}

An additional provision in the proposed legislation noted in the summary 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."\textsuperscript{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.\textsuperscript{5} Both civil penalties and injunctive relief would be available.\textsuperscript{6}

\section{Work vs. Home}

[Add the following text 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.\textsuperscript{7}

\section{Document Retention Policies}

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

\footnotesize
\begin{itemize}
  \item Id.
  \item Id. §2(b)(1).
\end{itemize}
A recent article by Nelson and Simek outlines a number of policies 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. 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.” Drawing on the work of Nelson and Simek, Kerschberg also discusses why companies should 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.

B. Discovery

I. Attorney-Client Privilege

[Add the following text 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, the court held that the attorney-client privilege

---


9 Id. at 5.


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. In *Williams v. District of Columbia*, 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.

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*, 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. This case especially useful because it 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 Con-

---


fidentiality of E-Mail Communications with One's Client, addresses the danger of third-party access to client communications. 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 of how he/she would like to be communicated with.

A quick search of the K&L Gates database of electronic discovery cases related to email in 2012 illuminates a number of common themes, including spoliation and sanctions; privilege and waiver; forensic examination of email accounts; cost shifting for processing email accounts, and motions for a protective order over email records, emails, text messages, and other related information from Yahoo and Verizon. 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 business community, so it still should be a matter of concern in the context of electronic discovery, as well as for overall information management.

2. **Possession/Custody/Control**

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

In 2012, the American Bar Association Commission on Ethics 20/20 has 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.24

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 ....”25 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;
- 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 accidentally transmitted, for example, as when an email or letter is misaddressed.26

---

26Id.
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.27

C. Cross-Border Issues

[Add the following text 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 released its resolution and report dealing with outsourcing.28 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 that is 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. (Former Comment [6] is redesignated as Comment [8] (Maintaining Competence).)

- 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.

III. Issues Arising Out of Impermissible Use of Email

A. Spam

2. The CAN-SPAM Act

a. What Is Covered

iii. "Hybrid" Messages

\[59\] [In footnote 93, correct the MySpace WL citation to "2007 WL 1686966."

v. "Initiating Transmission"

[Add the following text 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.\[20\] 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.\[30\]

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


\[30\] Id. at *1, 2012 U.S. Dist. LEXIS 25062, at *5.