Ombuds in Cloud of Exabytes--Understanding the Ombuds' Digital Trail

Craig B. Mousin, DePaul University

Available at: https://works.bepress.com/craig_mousin/9/
Ombuds in a Cloud of Exabytes — Understanding the Ombuds’ Digital Trail

CRAIG B. MOUSIN

ABSTRACT
This article examines Ombuds Standards of Practice as Ombuds increasingly rely upon electronic communication. It first explores the expansion of electronically stored information (ESI) due to the many different electronic devices Ombuds rely upon or interact with including computers, smartphones, and printers. It then reviews how novel legal issues caused by e-discovery — the search for relevant digital documents in litigation — will impact Ombuds. Finally, it offers Ombuds suggestions on managing and controlling ESI while raising the question of whether the International Ombudsman Association must review its Standards of Practice in light of these ESI developments.

KEYWORDS
Ombudsman, confidentiality, e-discovery, Standards of Practice, electronically stored information (ESI), digital records, record retention, Ombuds

It’s 2011; do you know where your records are? Ombuds have worked tirelessly to develop policies that protect confidentiality and minimize, if not eliminate, any records that might be used to breach confidentiality if they were turned over internally or provided to litigants in any court proceeding. As offices evolve from an environment when records could be locked up in a box and kept relatively secure to a world where electronically stored information (ESI) can be maintained on computers, cell phones, video recorders, thumb drives, lap tops, tablets, printers and scores of similar devices, new challenges confront Ombuds assurances of confidentiality. In addition to storage at an Ombuds’ institution, technology experts now tout the benefits of working in the cloud, where information will be stored on off-site servers, outside of the physical control of the Ombuds. Thus, Ombuds need to understand the full extent of their records or be lost in a cloud of information overload. How does one make sure all records are reasonably secure if the multiplicity of locations where records are produced and stored remains unclear? In addition, the expansion of ESI has placed demands on the legal system which will also force Ombuds and their institutions to respond. This article explores the diverse ways an Ombuds produces electronic records, intentionally or without knowledge, and offers some preliminary steps to address the electronic age’s innovations that increase the challenges to the Ombuds best practices.

Ombuds provide safe havens for Visitors to explore sensitive issues revolving around conflict, brainstorm options to access different conflict resolution strategies, and consider whether to become a whistleblower and the consequences of such action. Disclosure of records that reveal identity and/or issues undermines
confidence in Ombuds ability to fulfill their mission. Moreover, as the profession seeks to convince legisla-
tors or the courts that public policy supports the
establishment of an Ombuds privilege to not disclose
information, Ombuds must show consistent practices
and careful control over any documents or records
that must be maintained to prevail.

In examining these concerns, Ombuds face at least
three questions regarding the security of one’s office
information. The first concern addresses the scope
of the technology relied upon by Ombuds. Ombuds
must worry not just about securing records, but know
how, when, and where records are produced; how,
when, and where they may be transmitted; how,
when and where are records stored; and how, when
and where they are preserved and for how long. If
records are destroyed, how, when, where, and how
thoroughly are they destroyed?

A second concern involves identifying the parties that
might want to pierce confidentiality and what steps
must be taken to respond to those distinctive enti-
ties. In keeping with professional principles, Ombuds
seek to keep Visitors’ identities, conversations, and any
notes or memoranda about the Visitors confidential
from internal constituencies, to preserve the trust in
the Ombuds’ safe haven. Once a party seeks to litigate
against the Ombuds’ institution, the Ombuds will face
requests from outside the organization and, perhaps,
internally as General Counsel may request informa-
tion to assist in any defense of a lawsuit.

The third concern addresses a personal and profes-
sional issue. As technology offers seamless communi-
cation, Ombuds should evaluate how their personal
lives interact with their professional lives. Cell phones
may contain both professional and personal contacts
and information. Tablets may contain the bestselling
novel for leisure reading and the notes from a confiden-
tial call. Working from home may make one more
efficient, but what confidentiality questions are raised
when one sends emails or memos from one’s personal
home computer to one’s work computer or to others
with whom the Ombuds communicates electronical-
lly? Social media sometimes connect professional and
personal lives as well and raises similar concerns.

The International Ombudsman Association (IOA) has
established Standards of Practice (SOP) guiding Om-
будs responsibility regarding confidentiality. Ombuds
have sought to minimize or eliminate the produc-
tion of any records, but especially those that might
be held on behalf of the institution. To comply with
the SOPs, Ombuds must demonstrate that they have
taken all necessary steps to ensure confidentiality
regarding the production, maintenance, and destruc-
tion of records. Given the necessity of retaining some
information to properly fulfill one’s duties, the SOPs
further require that any such information retained be
kept secure and protected from inspection by others
or deleted pursuant to a consistent destruction prac-
tice. Securing, safeguarding and shredding records
remain key to ensuring that an Ombuds fulfills the
SOPs. These SOPs were prepared, however, in a time
when most records and information were composed
on paper. Today, Ombuds frequently produce digital
records. Although simply recorded as ones and zeroes
which collectively become a unit of information called
a byte, specialists now talk of exabytes of informa-
tion—enough storage to include the information
found in one trillion books. Fred Cates, an expert
in cyber security notes: “…more data than ever are
created and stored in digital form. As Stanford law
professor Kathleen Sullivan has written, ‘Today, our
biographies are etched in the ones and zeros we
leave behind in daily digital transactions.’”

Government officials now routinely access data that didn’t even
two decades ago. Some estimates suggest that
99% of all information is now stored electronically.
In 2010, the world’s ESI exceeded 2,000 exabytes — a
zettabyte of information. One estimate suggests
American business sends 2.5 trillion emails each
year. Wireless text messages exceeded two trillion in
2010. One hundred or more emails a day has become
standard professional fare. As electronic information
has expanded, so have breaches of private informa-
tion with over 250 million data records of U.S. citizens
breached through security lapses from 2005 to 2010.

Electronically stored information, thus, challenges
compliance with IOA’s SOP 3.6—what records are un-
der the control of the Ombuds? ESI “includes all infor-
mation stored in an electronic medium, including au-
dio and video files, e-mail messages, instant mes-
ges, voice mails, websites, word processing documents,
databases, spreadsheets, digital photos, information
created with specialized business or engineering
software and backup or archival copies of that same

\[ \text{volume 4, number 2, 2011} \]
information.”12 Backup systems, archiving systems, and computer programs all maintain information that add layers of record retention that did not exist when typewriters produced documents. Computers also contain metadata: “information about electronically stored files that is hidden in the files themselves. Metadata usually includes information such as the file’s creator, creation date, and dates on which the file was opened, read, modified or printed.”13

The Challenges ESI Poses to Ombuds

Our own institutions and society are simultaneously adapting to these changes. We need to be aware of the currents that are channeling those institutional and governmental responses in the technological and legal context as IOA articulates its professional standards.14 As National Institutes of Health Ombudsman Howard Gadlin warned us, our professional “principles were about professional practice standards and there is a difference between professional practice standards and the legal environment in which they operate.”15 Developments in the law, however, will impact Ombuds practice. The legal environment, specifically the influence of e-discovery — the search for relevant documents within a litigant’s ESI — raises issues that our own institutions must address, and simultaneously necessitates a response by the Ombuds profession. Litigation in the United States has primarily depended upon discovery of information prior to trial as an essential component of seeking the truth. The legal world, however, has only recently begun to grasp the extent of how seeking all relevant ESI has changed the landscape of contemporary court proceedings.16 When multiple employees working with their own computers and telecommunications devices become involved in a case, the cost of document retrieval, review, and production can conceivably run far greater than the potential liability of any one case, influencing institutions to consider critical legal decisions based on cost instead of actual liability. Thus, understanding the evolution of e-discovery litigation may assist Ombuds work within their own institutions to address confidentiality issues raised by ESI. At the same time, observing how other professions adapt to the burgeoning challenges of e-discovery may assist Ombuds resolve these practice issues.

Thus, an Ombuds has a responsibility to know who has access to all of those records and second, must work with General Counsel when a litigant requests ESI to understand what might be claimed as confidential and whether an ombuds privilege of confidentiality can be claimed.17 When legal action is commenced or reasonably anticipated, best legal practice calls for the General Counsel to issue a legal hold letter ordering the recipient to preserve all data subsequent to the receipt of the letter. Frequently, negotiations will take place to see what must be turned over in the litigation or other legal matter. If a reasonable record destruction policy calls for routine shredding of records and the policy is consistently followed, there typically would not be a duty to produce any record destroyed prior to any anticipated litigation. Information that was not routinely destroyed pursuant to an established policy may be subject to discovery. For an example of the extent of ESI subject to potential discovery, one court has ordered:

a party to provide a “copy of, or a description by category and location of, all documents, data compilations, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses.” More specifically, Rule 26(a)(1)(B) disclosures should “describe and categorize, to the extent identified during the initial investigation, the nature and location of potentially relevant documents and records, including computerized data and other electronically-recorded information....”

“Computerized data and other electronically-recorded information includes, but is not limited to: voice mail messages and files, back-up voice mail files, e-mail messages and files, backup e-mail files, deleted e-mails, data files, program files, backup and archival tapes, temporary files, system history files, web site information stored in textual, graphical or audio format, web site log files, cache files, cookies, and other electronically-recorded information.” Furthermore, the disclosing party should take “reasonable steps to ensure that it discloses any back-up copies or files or archival tapes that will provide information about any ‘deleted’ electronic data. (Footnotes omitted).18
General Counsel will work both with the institution’s employees to first determine whose ESI may be relevant to the particular case and then normally negotiate with opposing counsel over the scope of discovery, subject to the court’s approval. Imagine, however, if only five employees are subject to this discovery order, the extent of potential ESI records that must be reviewed.19

If in the course of subsequent litigation, the court determines that one side either failed to produce relevant information or destroyed information that should have been available, it can order sanctions against the party failing to comply, up to and including that the information was destroyed or failed to be produced should be considered adversely, permitting the implication of wrongdoing by the party failing to produce. The overall impact of destroying relevant electronic information comes under the term spoliation, which one court defined as “the destruction or significant alteration of evidence, or failure to preserve property for another’s use as evidence in pending or reasonably foreseeable litigation.”20 That court emphasized the dire effects of spoliation noting, “Aside perhaps from perjury, no act serves to threaten the integrity of the judicial process more than the spoliation of evidence….But, when critical documents go missing, judges and litigant alike descend into a world of ad hocery and half measures — and our civil justice system suffers.”21

Ombuds have longed for legislative and court recognition of a privilege of confidentiality similar to the attorney-client privilege. Attorney Charles Howard, who has litigated a number of cases defending Ombuds claims to confidentiality, has stressed that our practices will be examined closely when we seek the privilege to keep information confidential.22 The failure to protect records from destruction of ESI, even if unintentional, because an Ombuds did not know of all the ESI under his or her control would certainly undermine a claim of consistent practice in accordance with the SOPs. In addition to the negative consequences of spoliation, moreover, the overwhelming amount of information contained in ESI has resulted in inadvertent disclosure of material that might otherwise have been protected by a privilege. In Mt. Hawley Insurance Co. v. Felman Production, Inc.,23 for example, the lawyers for one party disclosed a large number of documents that might have been protected by attorney-client privilege. When the lawyers requested that the privilege precluded reliance on the documents at trial, the court held, in part, that because of the large number of disclosures, the lawyers’ failure to take reasonable precautions to avoid inadvertent disclosure, and the failure to promptly address the issue, the party waived the attorney-client privilege. Because the Ombuds claim to confidentiality has not yet received the same judicial and legislative protection offered under the attorney-client privilege, equivalent inadvertent disclosure of information an Ombuds might try to protect, would likely lead a court to require disclosure of that information. Thus, even if an Ombuds persuades a court to grant the privilege of confidentiality, inadvertent disclosure by an Ombuds would eliminate the victory by waiving the privilege. The rise of e-discovery raises the bar to require understanding of the size and shape of ESI produced by an Ombuds office and the care of its retrieval, review, and/or regular destruction prior to litigation being anticipated.

Understanding the Ombuds Digital Trail

A typical Ombuds day may generate very few traditional paper records, but leaves open the question of whether the Ombuds has lived up to SOPs 3.5 and 3.6 as seen in the following hypothetical. Preparing his breakfast, a certain Midwest Ombuds decides to check his electronic calendar to make sure he is aware of all his appointments for the day, proudly noting that the code he has established permits him to know which Visitors will arrive that day, but anyone looking at his calendar will see nothing but letters and numbers. He recalls that a Visitor asked to meet outside of the office for confidentiality purposes and he agreed to meet the Visitor at a local coffee shop. Walking the half mile to his train, he calls an Ombuds colleague at West Coast State University for some collegial advice. Given the time zone difference, he calls her cell phone and requests a copy of an article his colleague is writing regarding bullying in which he had provided her with some examples of egregious behavior. She emails him a draft of the article. Meanwhile, realizing that he is late for his first appointment, he calls the Visitor to inform her of his tardiness. After meeting the Visitor at the coffee shop, he takes public transit to his office. While on the train, he calls his office assistant to check in and confirm his arrival time, replies to two emails and responds to one of the voice messages on his cell phone. Leav-
ing the train, he walks through campus to his office building. He greets the security guard in his building's lobby and reminds the guard that an alumnus who does not have a current university ID card will be visiting later in the day. Arriving at the office, he turns on his computer, checks emails and downloads his colleague's article on bullying. He forgets about one voice message that he opened on the train, but notes that a colleague in Human Resources has sent him a confidential attachment. He opens the attachment, but realizing what it is, closes and deletes the email and attachment. He then responds asking that nothing be sent by email, indicating that he will walk over to her office and read the document in the HR office. He meets one Visitor in a conference room in a faculty office building which requires all entrants to swipe their university ID card. One Visitor asks him to copy a sheet with several phone numbers and contact information for the Ombuds to call when the Visitor is on vacation. As the Ombuds complies, he makes a mental note to destroy the sheet of paper once he no longer needs it. He gets an email from Facebook that concerns him — the Visitor he met at the coffee shop entered a note on her Facebook page lauding the Coasts who asks him to delete the draft research paper he has kept only one written note that is filed securely in a locked file cabinet, he believes he has lived one more day consistent with the IOA SOPs. The Ombuds heads for bed as his cell phone purrs with new messages, including one from his colleague on the West Coast who asks him to delete the draft research paper because she found a mistake where she had inadvertently included information that might disclose the identity of some Visitors. As our Ombuds drifts off, one small worry nags him — how many records has our well intentioned Ombuds developed in his one day of work that he must account for under the IOA SOPs? That small nagging feeling will soon overwhelm him when he realizes the avalanche of information that now is intentionally and sometimes unknowingly kept through his daily work through ESI.

Although this discussion does not exhaust all the potential records, there is little doubt that this hypothetical produced an extensive digital trail. Each time an electronic device was opened, the Ombuds produced an electronic record and a metadata chain of information regarding the activity itself. Voice messages are frequently digitized, and perhaps replicated in an email system, so that information has left a digital trail and when not deleted prior to normal back up policies, becomes a second set of records in the back up files.

The Ombuds should work closely with a team within the institution to determine the best methods for seeking the greatest protection for confidentiality. Working with the institution's document retention and destruction policy with added safeguards for increased confidentiality of Ombuds material should be an early step. Courts will examine if regular destruction policies are followed when no litigation is reasonably anticipated. The Ombuds should be aware of his or her institution's back up policy, if any, for electronic communications. Ombuds should consider deleting all electronic messages before back up occurs. Deleting emails and voice mails prior to back up on a consistent basis can also show good faith efforts to maintain confidentiality. Care should be taken, however, knowing that deleting destroys neither the message nor the metadata. Computer forensic experts can retrieve data that has been deleted unless additional wiping or destroying the hard drive itself eliminates the ESI. Deleting reduces the number of records maintained by the Ombuds, but does not delete all records. Encryption programs may be utilized to protect from internal review or outside hackers, but encryption still leaves "ones and zeroes": they may have to be unencrypted if they are left on hard drives or in archives prior to the anticipation of litigation. When computers or cell phones are replaced, care needs to be taken that the original hard drives or SIM cards are properly disposed of to prevent outsiders from obtaining information that is retrievable by forensic experts. 24

Did the Ombuds check his electronic calendar on his cell phone or home computer? Even if a code describes the appointments, has the Ombuds recorded the code and its keys on a written document prepared by computer? The Ombuds needs to know that just checking his calendar produces additional metadata
on those separate devices leaving a record that might identify the Visitor. Recall that metadata includes information that is stored on any computer every time a computer is turned on and a file opened.

Cell phones, especially smartphones, present particular problems. The ease of use and ubiquity of cell phones have led people to not use passwords for the phones themselves or the voice messages left on cell phones. A technique known as ID spoofing can enable another person's phone to disguise their phone and access voice mails. If passwords are not employed, the Ombuds places all his information at risk of possible theft. Moreover, cell phones leave a digital trail as they seek out cell towers leaving a trail corresponding with the actual Ombuds journey which can identify the location where the Ombuds met his Visitor at the coffee shop. When combined with the record of the calls, it could lead to the identity of the Visitor. Smartphones offer backup availability to the cloud — a server not owned by the Ombuds or the Ombuds' institution, but one where the Ombuds information is stored until needed by the Ombuds. Third parties may have access to that information through court ordered subpoenas or by hacking.

Relying on servers in the cloud may be the way of the future, but it places the responsibility on the Ombuds to reasonably know how to protect the confidentiality of the information stored in the cloud. Cell phones should be password protected with the ability to wipe out information if stolen or lost. As smartphones lead to millions of new apps, Ombuds should investigate whether a new app opens security concerns to their personal information. One app that advertised as a full service for owners with the bonus of encryption did not encrypt the metadata which included the file name. Thus, an unsuspecting Ombuds might innocently place a file name that provided identification which would not be protected under the apps encryption promises. Tablets raise many of the same confidentiality problems.

Modern copiers and printers often include a chip that digitizes all copies made on a machine. The Ombuds should use a copy machine or printer that does not have that option, or at least know that destroying the sheet of paper that had vacation phone numbers will not eliminate the record if the machine still has a digital record of the paper.

When the Ombuds stopped at the security desk, did a video camera record his image or the image of the alumnus Visitor later that day? If so, what is the institution's policy on maintaining and destroying the video recording? Likewise, the Ombuds and Visitor both swiped ID cards to meet at the faculty office necessitating that the Ombuds know the retention policy on tracking entries into university buildings.

The consequences of social media and confidentiality have just begun to be investigated. A Visitor’s use of social media may explicitly reveal communication with the Ombuds, but if privacy controls are not properly managed, may also disclose meeting locations and make more information public than either the Ombuds or Visitor would desire. IOA has already begun to discuss the use of social media and Ombuds practices.

Use of the cell phone, authoring the IOA Journal article at home, and receiving the email from the West Coast colleague all left a digital trail on multiple devices. Depending upon what the Ombuds worked on with a home computer or what emails might be sent or received from a personal email account, the Ombuds may have discoverable material, and therefore, General Counsel might put a legal hold on the home computer. Although it is less likely that a litigant could demand that a third party such as the West Coast Ombuds have her computer reviewed by a forensics expert, at least one court has ordered a forensic review of a non-party’s home computer to see if an email sent by the non-party to one of the litigants could be used as evidence in the trial.

This daily routine of an Ombuds production of ESI does not intend to frighten us into paralysis or back to the quill pen days when the unique paper record could be shredded to ensure confidentiality. With the size of some of our institutions, electronic communication may be the only way to permit access for some of our Visitors. Moreover, if history is any guide, most Ombuds will not be party to a lawsuit or subject to discovery. Under the SOPs, however, the Ombuds still has a duty to understand what records are under control of the Ombuds office. The intent, moreover, is to look for ways to encourage access and communication with maximum protection and control. Indeed, the Ombuds profession may have been a few steps ahead of others in understanding the complexity of
confidentiality and electronic communication. IOA’s professional training has long emphasized the importance of alerting Visitors to the possible breaches to confidentiality through the use of email. Just recently, however, the American Bar Association released a new Formal Opinion regarding an attorney’s duty to warn a client that if the client uses a company owned electronic communication device, there is a significant risk that the communications will be read by the employer or a third party.31 If such a policy exists, attorneys should warn their clients that all emails sent or received through the employer’s computers, cell phones, or telecommunications devices are subject to employer review, and therefore, face the potential that the attorney-client privilege would be unavailable to protect the communication from serving as evidence in litigation.

The American Bar Association’s Techshow and it has started to list standards for attorneys while seeking feedback from the profession.36 Several state bar associations have made it clear that attorneys have a duty to continue to educate themselves on the issues raised by new technologies. One scholar suggests that an attorney who litigates today and does not understand metadata, commits malpractice.37 The Seventh Circuit Court of Appeals has instituted a trial program for attorneys to understand the challenges of e-discovery. Its final point tellingly establishes a duty of continuous education regarding e-discovery.38 The state bar of Arizona includes within its Professional Responsibility rules, the following caveat:

…whether a particular system provides reasonable protective measures must be informed by the technology reasonably available at the time to secure data against unintentional disclosure.’ N.J. Ethics Op. 701. As technology advances occur, lawyers should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients’ documents and information.39

The Arizona bar further emphasized the duty of attorneys to “recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult available experts in the field.”40 Ombuds should have no less standard of reasonableness. IOA might consider gathering interested Ombuds to explore how Ombuds can best work with new technologies with integrity to our mission and continue to educate Ombuds regarding the use of electronic devices. The author is a member of the IOA Legal and Legislative Affairs Committee which is cur-

### Steps to Protect Electronically Stored Information

Given the scope of ESI, the following suggestions may help all Ombuds sleep better at night. First, develop a team approach with your information services staff (IS), your document retention and destruction policy staff, and your General Counsel’s office to anticipate issues and seek resolution. Work with your IS team to understand the many different ways you produce a digital record of your daily activities and what steps you can take to minimize unauthorized access as well as complete destruction of data as a routine course of business. Continue your education about how technology creeps into normal Ombuds practices and how one can encourage access without breaching confidentiality.34 Invite your IS team to find computer programs or apps that enhance security and organize the Ombuds’ ESI. Explore encryption programs that permit ease of communication. Follow the spirit of SOP 3.6 to use technology to secure all ESI produced by the office and enable efficient and effective review of ESI if the office receives a legal hold letter.

Know your institution’s document retention and destruction policy and, in communication with your institution’s staff, enhance it to meet the particular requirements of the Ombuds’ SOPs. Follow your document retention and destruction policy consistently to preclude any question that document destruction was done because of litigation, rather than as part of the normal practice.

Smartphones and tablets are easily lost or stolen. Ensure that information is encrypted; use passwords both for the device and for voice mails to avoid the spoofing problem. Investigate and add effective malware protection specifically for your smartphone. You may also download apps to block or wipe clean your smartphone if it falls into the wrong hands. Make plans to cover such possibilities knowing that human error remains one of the most vulnerable elements of computer security.35

Compare notes with colleagues in other professions such as health care, the law, and government who face similar issues. The International Legal Technology Standards Organization was recently established at the American Bar Association’s Techshow and it has started to list standards for attorneys while seeking feedback from the profession.36 Several state bar associations have made it clear that attorneys have a duty to continue to educate themselves on the issues raised by new technologies. One scholar suggests that an attorney who litigates today and does not understand metadata, commits malpractice.37 The Seventh Circuit Court of Appeals has instituted a trial program for attorneys to understand the challenges of e-discovery. Its final point tellingly establishes a duty of continuous education regarding e-discovery.38 The state bar of Arizona includes within its Professional Responsibility rules, the following caveat:

…whether a particular system provides reasonable protective measures must be informed by the technology reasonably available at the time to secure data against unintentional disclosure.’ N.J. Ethics Op. 701. As technology advances occur, lawyers should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients’ documents and information.39

The Arizona bar further emphasized the duty of attorneys to “recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult available experts in the field.”40 Ombuds should have no less standard of reasonableness. IOA might consider gathering interested Ombuds to explore how Ombuds can best work with new technologies with integrity to our mission and continue to educate Ombuds regarding the use of electronic devices. The author is a member of the IOA Legal and Legislative Affairs Committee which is cur-
Currently reviewing all SOPs. The Committee welcomes your ideas for ways to help all Ombuds enhance communication while maintaining protection of their data.

We live in a time when the ESI tsunami brings both blessings and curses. We can use the technology to assist our mission of assisting resolution of conflict and build a more peaceful world. At the same time, we can be so overwhelmed with the onslaught of “ones and zeroes” in our lives that we fear paralysis from attempting to leave no trail of ESI records. The courts have begun to recognize the overwhelming costs and burdens associated with e-discovery. They have sought proportionality and intentional cooperation between competing parties in the midst of litigation to preserve the court’s ability to find the truth in difficult controversies and limit the cost of reviewing “exabytes” of information to find that one email that sheds light on liability. Not surprisingly, seeking cooperative and peaceful resolution of conflict defines Ombuds work. Through collaboration with IS staff, document retention and destruction staff and General Counsel’s office, Ombuds seek a similar goal and bring a new level of security to the records we produce in our work.

At the same time, the ESI expansion may call for a review of the scope of Ombuds confidentiality. The profession may want to explore proportionality in terms of balancing access and working in partnership with one’s institution and Visitors to clearly express what can be kept fully confidential and what can be reasonably protected. At the very least, IOA may consider expanding the language we use to inform our Visitors about the confidentiality consequences of ESI. We can bring our resources to bear and exploit the new technologies without betraying our principles. Otherwise, if we hide our head in the cloud, we run the risk of disclosing far more information than we ever dreamed we possessed in the midst of all those “ones and zeroes.”

ENDNOTES

1 Two other additional groups may seek access to Ombuds information. Hackers, malicious or otherwise, may troll the data from Ombuds seeking confidential information or passwords that unlock other information. Finally, federal or local law enforcement may seek information or hacking by foreign governments may test the protection of an Ombuds’ ESI. These two additional areas also need to be examined, but are beyond the scope of this article. Nonetheless, some of the steps taken to safeguard ESI discussed in this article may also protect against these other risks.


3 IOA SOP 3.6 states in full, “The Ombudsman maintains information (e.g., notes, phone messages, appointment calendars) in a secure location and manner, protected from inspection by others (including management), and has a consistent and standard practice for the destruction of such information.” Ibid.


Craig B. Mousin


10 Losey and Baron, “Did You Know?”


14 This article addresses questions raised by the consequences of ESI and litigation within the United States, and thus, cannot address how other jurisdictions will be impacted. All Ombuds, however, need to be careful in protecting their own ESI. Moreover, this article does not provide legal advice, but raises questions about the impact of ESI and e-discovery that Ombuds should address with their attorneys or General Counsel.


21 Ibid, 258-9 (emphasis in the original). See also, Baron, Exabytes, *20-*29 describing how parties have to cooperate in the age of e-discovery.

22 Charles Howard, Organizational Ombudsman, 190-91, 292-95.


26 Although beyond the scope of this article, government surveillance has increased with less judicial oversight. As Fred Cates writes, “In years past, the government might physically follow a suspect or search his or her home, thereby creating at least the possibility (and often the legal requirement) for notice and an opportunity to object, whether through a judicial, legislative, or other process. Today, surveillance is far more commonly conducted through cell phone service providers or GPS transceivers, thereby eliminating the opportunity of individuals to be aware of, much less object to, the activity.” Cates, “Government Access,” 69.


28 Littler Privacy and Data Protection Practice Group, “What Does the ‘Year of the Tablet’ (or of The iPad) Mean for Em-
In my three block walk from my train to my office, I have counted at least 10 video surveillance cameras that appear to be operated by my institution. During the half mile walk to my train, entering the train station, and leaving, I have counted more than thirty other public and private cameras recording my daily commute. Had I met my Visitor at the coffee shop next to the station, our meeting may well have been recorded by the city police camera. My electronic card that I swipe for my fare each day records my movement on public transit and my colleagues’ toll payments on the expressway have been expedited by automatic toll collection while leaving an additional record of their daily commute.

See “Crystal Ball.”


Berryman-Dages v. City of Gainesville Florida, Case No. 1:10-cv-00177-MP-GRJ (N.D., D.C. Fl), 2011. The Order permitted a computer forensics expert to “image the hard drive…to search for the letter in question, and any related metadata, including the unallocated free space on the hard drive.” The court was also sensitive that private information on the home computer might be disclosed, and therefore, it ordered an independent expert conduct the review and ordered that all private information be kept confidential. Nonetheless, the e-discovery revolution will probably find lawyers constantly urging courts to enlarge the scope of subpoenas seeking ESI.

American Bar Association Standing Committee on Ethics and Professional Responsibility, “Formal Opinion 11-459, Duty to Protect the Confidentiality of E-mail Communication with One’s Client,” August 4, 2011. Such risk may also exist if a personally owned device links to a company’s network.

Find both internal and external resources to keep one up to date. For example, see the website sponsored by the Indiana University’s Center for Applied Cybersecurity Research for helpful tips. Accessed September 16, 2011. http://www.securitymatters.iu.edu.


Ibid.