ETHICAL ISSUES IN E-DISCOVERY, SOCIAL MEDIA, AND THE CLOUD

HON. RONALD J. HEDGES AND MAURA R. GROSSMAN, ESQ.
FEATURE: SYMPOSIUM: ETHICAL ISSUES IN E-DISCOVERY, SOCIAL MEDIA, AND THE CLOUD

This fall, members of the Rutgers Computer and Technology Law Journal (RCTLJ) had the great honor to sit down with the Hon. Ronald J. Hedges, former United States Magistrate Judge, and Maura R. Grossman, Esq., to discuss emerging issues related to electronic discovery.

Judge Hedges served as a United States Magistrate Judge in the United States District Court for the District of New Jersey from 1986 to 2007. Presently, he is the principal of Ronald J. Hedges LLC and is of counsel to Corodemus & Corodemus. He has extensive experience in e-discovery and managing complex litigation, and has served as a special master, arbitrator, and mediator.

Maura R. Grossman joined Wachtell, Lipton, Rosen & Katz as an associate in the litigation department in 1999 and was appointed as Counsel in 2007. She focuses her practice primarily on legal, technical, and strategic issues involving electronic discovery and information management, both domestically and abroad.

Judge Hedges and Ms. Grossman spoke at RCTLJ’s CLE symposium entitled, “Ethical Issues in E-Discovery, Social Media, and the Cloud,” on October 23rd, 2012. This discussion took place on November 7th, 2012.¹

RCTLJ: When opposing counsel is clearly inept when working with electronically stored information (ESI), for instance, choosing a poor set of search terms, what should an attorney do to uphold the interest of justice?

HEDGES: In a civil proceeding, an attorney has no obligation to do anything in the interest of justice. The attorney’s obligation is to represent his or her client and to conform to the Rules of Professional Conduct.² However, if the attorney knows that his or her adversary is doing something wrong and that the attorney has

¹ These comments reflect the personal views of the speakers and are not the views of any organization, firm, or client with which they are affiliated.
² See Model Rules of Prof’l Conduct R. 3.1 (2012); see also id. pmbl.
made an affirmative assertion to the contrary to the adversary or the court, then an obligation to do something arises.³

In a criminal proceeding there are obvious constitutional issues. For instance, a United States Attorney must see that justice is done. If she believes that an injustice will result due to the mishandling of ESI, she may have to step in and tell the court.⁴ The prosecutor must also think about the prospect of an incipient habeas corpus petition or other post-conviction action.

GROSSMAN: I agree with Ron; I am not aware of any ethical rule that requires you to help your adversary. Obviously you cannot make misrepresentations and both parties have an obligation to be competent.⁵ However there may be strategic reasons to educate or assist opposing counsel when it will benefit your client.

HEDGES: One thing I would suggest, if you are going to make that decision to help the other side, I think that this is a very important area to secure informed consent beforehand from your client.

RCTLJ: During our symposium you both emphasized the need for attorneys to be competent. Are judges also attaining and exhibiting the requisite technological expertise?

HEDGES: There is always a need for improvement and there does seem to be a distinction between federal and state judges. The federal courts have far more resources available to educate judges.⁶ For example, Maura and I just participated in a judicial training program on ESI. I do not know if state courts are able to provide such programs. However, there is no set level of expertise for any judge.

³. See id. R. 3.4.
⁴. Id. R. 3.8.
⁵. Id. R. 1.1.
⁶. For instance, the Federal Judicial Center, the research and education agency of the federal courts, provides a variety of educational programs for federal judges. See Federal Judicial Education Programs, FED. JUDICIAL CTR., http://www.fjc.gov/fsje/home.nsf (last visited Nov. 17, 2012).
Additionally, The Sedona Conference®, of which Maura and I are members, has recently made a new edition of the Sedona Cooperation Proclamation—Resources for the Judiciary that will help judges navigate through ESI issues during litigation.7

**GROSSMAN:** I think that just as in the bar, there are a range of capabilities; some people are extraordinarily talented and knowledgeable in this area and others are near the end of their legal careers and do not want to deal with ESI. The same is true for judges. But there are many educational forums where judges can go to learn about electronic discovery.8 There are also a number of bench books available from institutions like the Federal Judicial Center or from the New York State Court system, among other jurisdictions.9

**RECTLJ:** One of the greatest conundrums with e-discovery is the preservation of evidence. Can you provide some tips on how to preserve ESI effectively?

**GROSSMAN:** One of the first things you have to do is put a litigation hold in place.10 This means notifying custodians who have potentially relevant information to preserve it.11 Sometimes the information is not custodian-based and you have to speak to information technology (IT) personnel to preserve it. Once you put a litigation hold in place, the most important aspect is to understand what information you have and where it is located, which is often referred to as “data mapping.” The data map is essentially an inventory of where the information is located and whether it is reasonably accessible or not. This information will allow you to

---

11. See id.
have a good grasp on what you have and where it is to be found, and then you can move ahead with confidence.

**HEDGES:** I am not familiar with the procedures among the state courts. At the federal level, however, the parties must meet and confer and plan for discovery under Federal Rule of Civil Procedure 26(f) (FRCP). Then the parties must participate in a FRCP 16(b) pretrial scheduling conference with the judge. Both rules specifically talk about preservation. I think it is incumbent on lawyers to address these issues as soon as possible and to see what stipulations might be entered into. The parties should also go through their client’s ESI and sort out what is relevant and needs to be preserved from what is not and is therefore eligible for return to the retention cycle. This lets your client dispose of indistinct information and to define the scope of evidence preservation.

**GROSSMAN:** Often preservation decisions are unilateral decisions. Preservation may not be discussed at the FRCP 26(f) conference because the duty to preserve is triggered when there is reasonable anticipation of litigation. This is often well before the commencement of the lawsuit.

Furthermore, I think there are two schools of thought regarding preservation. First is the “save everything” mentality. The downside is that you spend a lot of time, effort, and money searching “everything” for potentially relevant information. Second is the “proportionality” or “reasonableness” approach where the client makes a thoughtful decision about what is most likely to be probative and contribute to the resolution of the dispute, without getting overly concerned about the fourteenth copy of something very peripheral. The latter approach can be risky at

---

13. **Fed. R. Civ. P. 16(b)**
the beginning of the matter, however, when all the issues have not fully emerged, as you may fail to preserve something that should be preserved because you were not aware of its relevance at the time.

**RCTLJ: Would you say that a good shorthand to follow is notification, assessment, and data mapping?**

**GROSSMAN:** They are essentially performed at the same time. When you notify the key custodians to preserve ESI you are also assessing what they have and what you need. In an ideal world, the data map is part of the records management process. Your client needs to get its house in order before litigation commences.

**HEDGES:** The big debate is how the concept of proportionality is related to the initial decision to preserve. The proportionality rule is found at FRCP 26(b)(2)(C) and has counterparts in various states. The client only has to preserve what is needed for litigation. Since discovery is so broad, it is hard to make decisions about proportionality before you see a pleading.

**GROSSMAN:** We now have some case law on that issue from the Southern District of New York. My earlier point was that the way in which you apply it can be very tricky. I wrote an article with Gordon Cormack in The Sedona Conference Journal on this issue. Proportionality is a little like driving on a highway with a sign that says “Drive at the speed that is appropriate depending on what time you need to get to your destination, the weather and driving conditions, the price of gas, and so on,” rather than at “55 MPH.” Unless you have a conversation with opposing counsel, you do not always know what to preserve, but parties are often hesitant


17. FED. R. CIV. P. 26(b)(2)(C).
18. See id.
to have that conversation. There are some judges who have said that proportionality applies to preservation, and that you should not spend $100,000 preserving ESI in a $50,000 case, but the application of proportionality in practice can be very challenging.

RCTLJ: Should attorneys actively instruct their clients that their electronic records should be preserved, including communications like instant messages and text messages?

GROSSMAN: The answer to this question is not "should," but "must."21 Attorneys have an obligation under the common law as well as ethical obligations to instruct their clients to preserve potentially relevant evidence in all forms.22 This includes evidence of any kind, including text messages, social media postings, and SharePoints.23

RCTLJ: What issues does telecommuting present for preserving ESI?

HEDGES: Telecommuting presents a number of challenges. There is a new phenomenon which sees employees using their own computers for work-related purposes, that has been given the name, "Bring Your Own Device" (BYOD).24 People are more productive and organizations can get more out of employees if they allow them to use their own devices at, for example, remote locations or odd hours.25 The first problem is if the organization does not have a tight policy on what is allowed or not allowed, it may not know

22. Id.
23. Id.
where its data resides. If the data resides on a personal device, such as the smart phone I am using now to talk to you, the question becomes: “Is there relevant information on there? How do you get it?” Federal laws limit how some of that information can be accessed. The organization has to deal with employee confidentiality issues and personal information that may be comingled with relevant ESI. The second problem is, what are the consequences? If the employee leaves his employment, how does the organization know what is on the employee’s personal device and how does the organization obtain that information, especially when subject to a litigation hold? What discussions occur between the employer and almost-former employee about how to get the information and how to avoid exposing personal information?

GROSSMAN: I agree with Ron that, in general, telecommuting and BYOD can raise complex issues. Some of those same issues exist today when I use my BlackBerry for both personal and business use. When people comingle personal and business data on devices, issues such as possession, custody, control, and privacy get complicated. But it is a fact of life that people work from home using their iPads or use only one cell phone for all purposes. As a practitioner in the digital age, we have to deal with this and develop appropriate organizational policies.

RCTLJ: We are conducting this interview one week after Hurricane Sandy pummeled the East Coast. Should organizations secure disaster recovery backups for ESI and, if so, how long should those records be maintained? Would the lack of disaster recovery backups warrant sanctions against the client?

GROSSMAN: One of the problems that has emerged and has been eye opening to law firms and their clients is that even if there

26. Horbaczewski & Raether, supra note 24, at 75-76.
27. For an examination of recent decisions on this issue, see Christina Michelle Jordan, Courts Address Preservation of Personal Electronic Device Data, LITIGATION NEWS (July 5, 2012), http://apps.americanbar.org/litigation/litigationnews/top_stories/070512-electronic-device-data.html.
are disaster recovery backups, if they are stored on the same premises as the original computer, they may drown at the same time as your other data. Should there be off-premises disaster backups? Similar questions probably came up following Hurricane Katrina.28 I think it depends on the circumstances whether it creates a subsequent spoliation problem. It depends on whether these backups were created for routine business purposes or for the purposes of preservation. If it is just routine storage by the client and there is no litigation hold in place, it may be annoying or troublesome to lose the data, but there is no spoliation problem. It might be different if these backups were for the purposes of a litigation hold. A flood would not be considered intentional, or probably even negligent, but a court may still impose remedial measures to make sure that the opposing party is not prejudiced by the loss.29

HEDGES: This situation makes me think about reasonableness. Is it reasonable to take precautions against a storm like Hurricane Sandy? Yes, of course, to the extent such a “superstorm” is foreseeable. Now the question is what are reasonable measures? We have had so many instances of flooding in the Northeast in the last few years that you cannot simply keep your ESI in the basement and reasonably believe that all will be fine.30 I think that conduct reasonably could encompass the backup in an alternative location. The question is what are we doing now after this storm? What are we doing now that people are recovering? I think there

29. See generally Michael R. Nelson & Mark H. Rosenberg, A Duty Everlasting: The Perils of Applying Traditional Doctrines of Spoliation to Electronic Discovery, 12 RICH. J.L. & TECH. 14 (2006) (examining the dilemma in corporate America today of whether to retain vast quantities of ESI to avoid the possibility of potential spoliation sanctions despite uncertainty that such ESI will ever be necessary for litigation).
30. See generally Jill P. Capuzzo, Getting Used to Wet Basements, N.Y. TIMES, Apr. 11 2012, at RE8 (discussing the many floods New Jersey residents have endured over the past decade and that a rise in sea levels may lead to more flooding than ever before throughout the state).
will be a lot of different responses if the question is posed at a regulatory hearing, legislative hearing, or in a courtroom. I am sure we will get a lot of different answers. Ask us that question in a year.

**GROSSMAN:** Also, creating full or incremental backups and storing them in multiple locations is very expensive. What about a public school? Are they supposed to have off-site copies and create backups every day? Who is going to pay for that? We have to be realistic.

**HEDGES:** What it all comes back to is that we need to realize that we keep a lot of information that we do not need to keep. Maybe this will make us step back and ask how much information we keep and why we keep it. For example, when should we make the backup file and how long should we keep it. I think the answer is we keep it because we are waiting for some disaster to happen. I understand that as the whole theory for backups. If the predicted date of the disaster has passed, why keep the backup? Everything we have after Sandy is available now. If everything has been restored, why are we keeping the backup? I do not think backup tapes should be a big issue. Maura?

**GROSSMAN:** About how long to preserve them? Technically the purpose of backup tapes is not to archive information, it is for disaster recovery. If your system goes down tomorrow, you can bring it back up. Under that view of their purpose, one does not need to keep them for terribly long, perhaps thirty days. Some businesses, however, feel the need to keep them for much longer. It depends on what you are using the backup for.

**RCTLJ:** Are there any foreign privacy policies regarding social media or the cloud that you believe are a good model for the United States, either federally or for individual states? For example, the Canadian Supreme Court recently ruled that
employers have no right to look at an employee’s Internet history. 31

HEDGES: The answer depends on which country, and whether or not it is a common law or civil law one. 32 The Canadian decision is based on Canadian common law. 33 The civil law countries of Europe have a strong view about personal privacy. 34 This is likely based on the persecutions and genocide of the Holocaust. We in the United States do not see privacy in the same way. We do have “sectoral” privacy, such as the protection of health information through the Health Information Portability and Accountability Act (HIPAA). 35 On the federal side, I doubt we will see legislative successes in broadening the scope of privacy. We may see some sectoral successes. Another concern regarding this topic pertains to issues with data from other countries. Many countries restrict receipt of access to personal data.

GROSSMAN: There are huge differences between the United States and other countries, particularly civil-law countries, not only in the way discovery is conducted, but also cultural differences in the way that privacy is viewed. 36 Other countries do not have the

32. See id.
33. See id.
36. See Ellen Relkin & Elizabeth O. Breslin, Hiding Across the Atlantic, 48 TRIAL 14, 15 (June 2012) (noting that the United States’ broad discovery rules conflict with European data privacy laws which require a higher standard of relevance); see also Rolf Stümer, Some European Remarks On a New Joint Project of The American Law Institute and UNIDROIT, 34 INT’L LAW. 1071, 1075
breadth of discovery that we have in the United States. Other countries are also much stricter regarding personal privacy. When I turn on my computer in the morning, I receive an alert that says that the organization is privy to the information I create or receive. We all often think that even though it says that the company has access to everything we do, it does not actually mean that. In other countries, the message does not show up. The employees’ use of the computer is private. That said, over time, there has been more of a convergence of the two positions which were initially polar extremes. There is a movement towards narrowing the breadth of discovery in the United States, although it will never be as narrow as it is in the European Union. But there is a movement to rein it in, simply because the volumes are getting out of control. There is also a movement towards more privacy in the United States, because people have realized that companies like Target record what you are buying and may be “crunching” that data to figure out what is going on in your life. For example, depending on what you buy, they can figure out that you are pregnant and start sending you coupons for diapers. This makes people uncomfortable.

RCTLJ: Are attorneys seeking guidance for ethics matters from local bar associations often enough, or is the bar playing “fast and loose” with the application of existing ethics rules to novel social media situations?

GROSSMAN: We should start with the assumption that most lawyers are not unethical. Most lawyers are ethical, but they may or may not be competent in e-discovery. If they are making mistakes, the mistakes are generally not intentional. There are hotlines to provide help for attorneys. New York has one that receives many

(Fall 2000) (comparing the different functions discovery plays in the American, German, and Italian legal systems).


calls that deal with questions which are technical in nature. The average attorney is probably not using it, but the hotline does exist. There is a lot of distrust right now in discovery. People are assuming that the other side is out to withhold information, but it may be like plane crashes. Most planes land safely, but we only hear about the crashes. Similarly, we only hear about the disaster cases where parties destroy or withhold information intentionally.

HEDGES: Many attorneys go about business as they always have. When an attorney comes across ESI, he tends to apply the ethic rules he knows. However, there is a disconnect. For example, if you are working from a coffee shop with Wi-Fi access, others may have access to your confidential information. Lawyers need to be educated on technology-related matters.

GROSSMAN: Many lawyers do not fully appreciate all of the implications of new technology.

RCTLJ: Is it unethical to use cloud servers for storing ESI?

GROSSMAN: It is not per se unethical. A whole slew of ethical opinions have concluded this, provided that: (1) the practitioner does appropriate due diligence to protect the privacy, security, and confidentiality of the information and (2) the practitioner stays abreast of technological changes. While informed consent of the client is not a requirement, it is a good idea. If the practitioner is not an expert in cloud computing, he or she should consult with a security expert and understand that it requires a lot of thought when it comes to contracting for cloud services, for example, ensuring that you can preserve and get your data back for the purposes of electronic discovery.

QUESTION: Is there a chain of custody issue when evidence is stored in the cloud, especially when the storage server may be out of the United States?

GROSSMAN: Chain of custody is not necessarily the key issue, but rather data privacy and protection is. If the server is one of the countries that have data privacy laws that do not allow for export, then how can you get the information without violating that law?

HEDGES: Rephrase the question. “What is an original and, if the original is electronic, how do you authenticate the ESI?” Does the location of ESI somewhere in the Internet pose particular challenges? Lorraine v. Markel American Insurance Company talks about how various forms of ESI may be admitted into evidence. The answer is to simply print out the document and have your client testify that the document is accurate. We are moving more and more into a world where we do not have physical contracts. You can just print the electronic document out and move it into evidence. The question is, what do you do to challenge admissibility? The Federal Rules of Evidence are not meant to exclude information. I think we need to take a step back and ask the question: “Whatever medium the document is on, how do we admit it under the appropriate rules of evidence?” The best guidance comes from Lorraine decision.

GROSSMAN: There is a slightly different issue that sometimes comes up. When data is put in a cloud, it may be maintained in a different form than the original. The metadata may be altered. If metadata is an important issue in the case, you may need the data in its native form to avoid authentication issues. But generally, Judge Hedges is correct—it is about laying a foundation to get it admitted. In criminal matters, for example, if I am storing child

42. See Popović, supra note 37 at *5.
pornography in the cloud rather than on my laptop, does that pose particular issues for the government in proving its case against me?

**HEDGES:** It depends on how the Government gets access to the material—warrant or application. Then it is about how it can be used against you. There may be constitutional or statutory restraints against the government getting information from the cloud.\(^4^4\) There really are not many decisions on point and the decisions conflict.

**RCTLJ:** Yesterday was Election Day. In New Jersey, Governor Chris Christie has permitted citizens displaced by Hurricane Sandy to vote via e-mail.\(^4^5\) If an employee votes from their work computer does the employer then have a right to access the employee's vote?

**HEDGES:** If the Governor's Executive Order allows a voter to vote electronically, the voter can presumably vote from work. There are confidentiality issues here. I do not know that there is an answer per se. We may need to look to terms governing internet access in employment agreements.

**GROSSMAN:** That information may very well be in the internet cache of the computer. If the law firm has a policy that says they have access to all the information stored on the computer, then the firm would have access to that information.\(^4^6\) Unless the ballot was encrypted, it would be possible for that information to be accessed. There is no rule or regulation that I am aware of that prohibits a corporation from accessing that information if the corporation has a policy that allows them to see it.

**RCTLJ:** Ms. Grossman and Judge Hedges, thank you very much for your insights and perspectives on developing issues in electronic discovery.


Edited by Kersten Roehsler Kortbawi* & Henal Patel**

** Managing Editor, Rutgers Computer and Technology Law Journal. J.D., Rutgers School of Law—Newark, 2013; History/English, summa cum laude, Rutgers, the State University of New Jersey.