Boston University
Journal of Science & Technology Law

Symposium

Lawyers Online:
Discovery, Privilege, and the Prudent Practitioner

Steve Bauer, David Byer, John H. Jessen, Judge William G. Young,
Julius Levine, and Donald G. Leka

Table of Contents

Lawyers Online: Discovery, Privilege, and the Prudent Practitioner†

Steve Bauer, David Byer, John H. Jessen, Judge William G. Young, Julius Levine, and Donald G. Leka

Left to right: Steven Bauer, John Jessen, Donald Leka, David Byer, Judge William Young, and Professor Julius Levine

 Cite to this symposium as: 3 B.U. J. SCI. & TECH. L. 5. Pin cite using the appropriate paragraph number. For example, cite the first paragraph of these proceedings as: 3 B.U. J. SCI. & TECH. L. 5 para. 1 (1997) (comments of Steven Bauer). These materials are proceedings from the fifth session of the Internet Law Symposium held at Boston University School of Law on February 14, 1996. For materials from the other sessions see, 3 B.U. J. SCI. & TECH. L. 1-4 (1997).

Steve Bauer:[1]

1. Welcome to the fifth session of the Internet Law Symposium held at Boston University School of Law. The Symposium was co-sponsored by the law firm of Testa, Hurwitz and Thibeault and the Center for Law and Technology at Boston University School of Law. Previous sessions addressed the impact of the Internet[2] on business in terms of products and services, and risks and liabilities. Specifically, these sessions dealt with business initiatives,[3] intellectual property,[4] censorship,[5] and financial services.[6] Today's session is devoted to the practice of law and the issues we face as lawyers giving advice, or as clients taking advice. David Byer, an expert in complex technical litigation, will function as moderator.

David Byer:[7]

2. With the growth of the Internet over the last year, it behooves us all to think about the Internet in several different ways. First, think of it as a research tool. What can we do with the Internet prior to filing a lawsuit, or during an investigation that might influence our decision to file a lawsuit? We can use the Internet as an evidence gathering tool. On the other hand, the Internet may be an engine for the liability of our clients. Therefore, we need to know the scope of that liability and ways to counsel around it. In addition, because we litigators live concretely, the discovery phase of litigation takes on an entirely new cast when we

---

1 Steven M. Bauer, Esq. is Co-Chair of the Patent and Intellectual Property Practice Group at the Boston-based law firm of Testa, Hurwitz & Thibeault, and specializes in the protection and enforcement of intellectual property rights, including technology and software licensing.

2 The Internet is a "global system of networked computers that allows user-to-user communication and transfer of data files from one machine to any other on the network." JOHN DECEMBER & NEIL RANDALL, THE WORLD WIDE WEB UNLEASHED 6 (2d ed. 1995). References to the "Internet" are capitalized. *See* WIRED STYLE: PRINCIPLES OF ENGLISH USAGE IN THE DIGITAL AGE 24 (Constance Hale ed., 1996) [hereinafter WIRED STYLE].

3 Symposium, *Internet Entrepreneurs, New Traffic Patterns, and Policy Issues*, 3 B.U. J. SCI. & TECH. L. 1 (1997).

4 Symposium, *Protecting Software and Information on the Internet*, 3 B.U. J. SCI. & TECH. L. 2 (1997).

5 Symposium, *Pornography: Free Speech or Censorship in Cyberspace?*, 3 B.U. J. SCI. & TECH. L. 3 (1997).

6 Symposium, *Financial Services: Security, Privacy, and Encryption*, 3 B.U. J. SCI. & TECH. L. 4 (1997).

7 David Byer, Esq. is a partner at the law firm of Testa, Hurwitz & Thibeault where he practices intellectual property.

think about internal systems, such as intranets,[8] servers,[9] version control software,[10] backups,[11] and archives[12] as well as external systems, such as the Internet, e-mail,[13] and other electronic forms of documents and data.

3. One study suggests that in the last seven years, business-to-business mail has declined 35 percent.[14] Some argue that the reason for this decline is that business-to-business mail is now done through e-mail. Now, just as you could discover the letters written between companies, so too could that e-mail be discoverable in litigation. Another study suggests that in the year 2000 there will be 60 billion e-mails sent.[15] That is a significant number of discoverable documents. To help us understand this new electronic age, John Jessen will begin with his perspective. Mr. Jessen is the Managing Director of Electronic Evidence Discovery, Inc.[16] He is perhaps the most famous member of our panel, having the distinct pleasure of being mentioned in *Forbes* and seen on *60 Minutes* discussing e-mail privacy issues.[17] Mr. Jessen is an expert in the area of electronic evidence

---

8 An intranet is a private network designed strictly for internal company use. *See* WIRED STYLE, *supra* note 2, at 50.

9 A server is a computer that when accessed transfers stored data and files to other machines on a network. *See id.* at 55.

10 Version control software provides a database that keeps track of the revisions made to a program by each programmer involved. ALAN FREEDMAN, THE COMPUTER GLOSSARY: THE COMPLETE ILLUSTRATED DESK REFERENCE 538 (1993).

11 A backup is a duplication of electronic data for storage. *See* WIRED STYLE, *supra* note 2, at 156.

12 An archive is a backup copy of data, often compressed to conserve storage space. *See* FREEDMAN, *supra* note 10, at 20.

13 Electronic mail, or e-mail, is an electronic communications medium that permits the exchange of text, information, and files via local area networks or the Internet. *See* THE INTERNET INITIATIVE: LIBRARIES PROVIDING INTERNET SERVICES AND HOW THEY PLAN, PAY, AND MANAGE 194 (Edward J. Valaukas & Nancy R. Johns eds., 1995) [hereinafter INTERNET INITIATIVE].

14 *Hearings on U.S. Postal Service Oversight Before the House Comm. on Post Office and Civil Service*, 103d Cong. 432 (1994) (testimony of Michael Motley, Associate Director, General Accounting Office).

15 *See* Scott Dean, *E-mail Forces Companies To Grapple With Privacy Issues*, CORP. LEGAL TIMES, Sept. 1993, at 11.

16 Electronic Evidence Discovery, Inc. is a provider of electronic discovery services. For more information on Electronic Evidence Discovery, Inc., see <http://www.eedinc.com>.

17 *See* Jeffrey Young, *Spies Like Us*, FORBES, June 3, 1996, at 70; *60 Minutes* (ABC television broadcast, June 16, 1996), *available in* LEXIS, News Library, Script File.

discovery and on the use of the Internet as a litigation tool. He has more than 16 years experience in this field.

John Jessen:[18]

4. Today, I will discuss the use of electronic data as a discovery tool in litigation. Specifically, I will talk about the Internet as a discovery tool and a source of litigation liability. I want you to keep in mind that electronic discovery includes all electronic data: word processing files, spreadsheets, databases, and the Internet, as well as bulletin board[19] service providers such as CompuServe,[20] America Online,[21] and others. There are a few facts that provide a basis for this new electronic discovery environment.

5. First, electronic data is being targeted now by regulatory agencies[22] and by litigators.[23] Targeting is the key word. No longer is electronic discovery a passive event where it often did not matter if electronic data got turned over at all. Today we are seeing specific requests for electronic data sets, and stringent efforts are being taken to ensure production. Rule 30(b)(6) depositions[24] are being taken of e-mail administrators, backup administrators, help-desk personnel, and electronic database managers. Any number of different depositions are being taken that go right to the core of what a computer system is and what it looks like for a targeted entity.[25] It is no longer a question of whether or not electronic data will be targeted in a given litigation. Now it is a question of when and how it will be done.

---

18 John H. Jessen is the Managing Director of Electronic Evidence Discovery, Inc.

19 A bulletin board provides access to programs and files, electronic mail, and in some cases connections to the Internet. *See* INTERNET INITIATIVE*, supra* note 13, at 193.

20 For more information on CompuServe, see <http://world.compuserve.com>.

21 For more information on America Online, see <http://www.aol.com>.

22 For example, the Securities and Exchange Commission and the Environmental Protection Agency take electronic filings. *See* 17 C.F.R. § 232.501 (1996) (securities filings); 40 C.F.R. § 75.64 (1996) (hazardous air pollutant emissions reports).

23 *See generally* John H. A. Pooley & David Mishaw, *Finding Out What's There: Technical and Legal Aspects of Discovery,* 4 TEX. INTELL. PROP. L.J. 57, 59-60 (1995) (explaining how lawyers are using electronic data discovery to search for and obtain information).

24 FED. R. CIV. P. 30(b)(6).

25 *See* Armstrong v. Executive Office of the President, 1 F.3d 1274, 1280 (D.C. Cir. 1993) (finding e-mails subject to the Federal Records Act).

6. Second, court rules and state laws now allow for electronic discovery,[26] and the legal arena is realizing computers hold tremendous amounts of information. The California legislature will consider an electronic data discovery bill[27] intended to open the door to electronic discovery. This type of legislation demonstrates that computers have become so commonplace that most lawsuits involve the discovery of some type of computer stored information. That is not a vendor, consultant, or attorney talking; that is a state legislature saying that electronic data will be used in discovery. The legislation also demonstrates that the development of new technologies for using, storing, and transmitting information allows parties to test the rules of disclosure by using these new technologies as a basis for holding information otherwise discoverable. These are all dramatic statements about electronic data and its use in the discovery process. There is little doubt that they will further open the door to electronic discovery.

7. Third, the processing tools required to make use of vast amounts of electronic data exist in the form of powerful, inexpensive microcomputers. This equipment did not exist 10 or 15 years ago. Today, we have hardware and software tools that can be used to identify, locate, retrieve, and review large volumes of disparate data sets.

8. Fourth, the courts are approaching electronic data in a way no one could have anticipated, by allowing discovery of backup systems consisting of hundreds of thousands of tapes. I was working with clients that had 600,000 backup tapes frozen by a court order. For a period of time they had to make backups everyday, saving each backup tape as well. That is obviously a very dramatic example, but we are seeing that type of activity starting to take place in many different cases.

9. Fifth, users of computer systems are going to put things into electronic mail and electronic data sets that no one ever dreamed would be possible. I do not care what you have seen in the paper over the years, the content of electronic data files -- especially things like electronic mail -- will shock and amaze. The mind-set that is brought to the electronic world by the average user forces them to take computer use in a very casual way. They often put things into a computer system that they would never put into writing on a real document. Users of e-mail systems believe that electronic mail is an ad-hoc, short-term, direct communication tool that provides private communications and allows for permanent deletion of messages when needed. They neither understand system backups, nor believe that electronic mail gets backed up. They believe that if anyone got their hands on a piece of their electronic mail, privacy rights prohibit disclosure.[28]

---

26 *See, e.g.,* N.C. GEN. STAT. § 1A-1 (1993) (comment to Rule 34 in the 1975 amendments clarifying that documents include electronic data compilations).

27 A.B. 3281, 1995-1996 Leg. Sess. (Cal. 1996).

28 *See* Joan Indiana Rigdon, *Management: Curbing Digital Dillydallying on the Job*, WALL ST. J., Nov. 25, 1996, at B1 (noting employers' increasingly frequent examination of employee e-mail).

10. From a technical and a legal standpoint, the attitude of the majority of e-mail users is wrong. When asked why they use e-mail, most answer that it replaces the telephone. What we have in today's environment are people bringing an informal, telephone call mentality into a medium that has permanent, or at best, semi-permanent retention. That can be dangerous or valuable if you happen to have your discovery hat on and are looking for informal, contemporaneous information about what is happening in the organization.

11. In addition to electronic mail systems, there are other electronic platforms that can play roles in discovery in ways that users have not comprehended. Voicemail[29] is an example of an existing technology that is going through a rapid change. Historically, voicemail resided on leased third-party stand-alone systems that were not backed up and from which data could not be easily retrieved. Today, virtually every major voicemail system is being converted or migrated to the computer platform. Voicemail is becoming just another program running on the computer.

12. Since it was very difficult to get voicemail in the past, it did not show up in litigation in large numbers or with great frequency. Now, however, since the voicemail message is just another file on the computer, it is widely available. We are seeing large volumes of electronic voicemail messages backed up, placed on floppy diskettes, and even being appended as files to electronic mail messages and being sent around the company.

13. New technologies are coming into play that are having a profound impact on the types and quantities of information being captured and stored, and, accordingly, on the discovery process itself. Videomail[30] is an example of new type of technology that is being brought into organizations with greater frequency.

14. It is bad enough when users type in electronic mail without an understanding of what is happening to the data, or leave a voicemail message on a computer without realizing that they are creating an electronic file that is probably going to get backed up that night. Now imagine those users in front of a camera, recording themselves talking, singing, or dancing and sending that electronic video clip to their friends with the belief that is private and under their control. Like the voicemail we discussed earlier, these video clips become electronic files and are subject to all of the operations like backup, copying to floppy diskettes, being sent as an attachment, and being replicated on many systems in many places.

15. I recently had a case involving the discovery of electronic data such as videomail clips. One side had been asking for an answer as to why the construction of their building was behind schedule and over-budget. Someone found a video clip

---

29 Voicemail involves the electronic recording of telephone messages that can be forwarded, replied to, and saved. *See* WIRED STYLE, *supra* note 2, at 89.

30 Videomail involves the electronic recording of video clips of a conference among several users provided by video cameras and monitors. FREEDMAN, *supra* note 10, at 509, 539.

on which the construction foreman on the other side was corresponding with his boss over the videomail system. He told his boss, "They want an answer, here's their answer," and he dropped his pants in front of the camera. This is the type of thing that people do when they are using technology without understanding what happens to that video clip as a data set on a computer system.

16. I want to specifically address the Internet. What is the Internet? Even people who deal extensively with the Internet have no good answer to this. There are many competing interests today that are rapidly reshaping the Internet, its mission, and its future. The Internet may best be thought of as an ad-hoc collection of computer systems that shares information and creates an infrastructure for electronic data to be created, stored, and transmitted instantaneously. If you have ever had the chance to look at an Internet electronic mail message, you may have wondered what all the strange looking names and codes were at the beginning of the message.[31] These are all of the places that the message has visited before it got to you. At each of those places that message could have been stored or archived, or read by others. This creates an interesting puzzle in the discovery process.

17. Although businesses and individuals have been rushing into the Internet environment, there is little agreement as to why this is happening. What is the business reason for allowing access to the Internet? What are all of these people going to do once they get there? That confusion creates opportunities in the legal arena. Electronic data sets that contain tremendous amounts of current and historical data can create liability.

18. The Internet is used by attorneys for communication with their offices and clients. As with electronic mail, the Internet is a communication device and a transfer mechanism. Marketing and business development is being done over the Internet by attorneys through ad-hoc generic homepages,[32] and specific, targeted marketing campaigns. It is being used to research travel options and to search for and gather general business information.

19. In the discovery setting, we see the Internet as a mechanism for researching specific organizations, clients, and adverse parties. It is important to go out and conduct your own review on the Internet so that you can find out what others would discover about your client if they conducted such a search.

20. You can build tremendous profiles of individuals and corporations from the Internet. You can retrieve information about the adverse party's systems, data sets, and organizational structure, and use all that information in a preliminary

---

31 Those messages are called headers. In addition to identifying the route traveled, headers also identify other recipients and the time, date, and location where the message was sent. *See* Katie Hafner & Matthew Lyon, *Talking Headers*, WASH. POST, Aug. 4, 1996, (Magazine), at 13, 21.

32 A homepage is a document on the World Wide Web that provides information about a business, organization, or specific field of interest, and contains links that direct the user to other information about, or relevant to, the subject of the homepage. *See* ACLU v. Reno, 929 F. Supp. 824, 836 (E.D. Pa. 1996).

fashion to determine if electronic data is relevant to a given matter. This includes analyzing the adverse party's or your client's homepage. Huge collections of data are available from online newspapers and magazines, and from vendors putting out electronic press releases.

21. Be cautioned, however, that others may be watching the Internet. If you are out asking online questions, a profile can be built of what you are looking for. A search can be conducted on your name or on the name of your law firm. Proper review and analysis can indicate what you are asking about, leading to a determination of what you are trying to accomplish in the litigation. Keep in mind that you are in a public forum when you are on the Internet; information about your activities may be retrievable by others.

22. Through depositions and interrogatories lawyers are getting detailed information about access to electronic databases and mail lists of registered employees. We are seeing targeted efforts to find key players in the information systems arena and depose them about the hardware, software, data, policies, and procedures. They are even being asked what online chatgroups,[33] and usenet newsgroups[34] they belong to.

23. What are the privilege issues involved in using the Internet? To avoid waiving privilege, take precautionary steps. When you send electronic mail onto the Internet, it being placed onto a public forum. Although there is no reported case law in this area yet, privilege could be held to be waived if you have not taken additional steps to ensure confidentiality and security. One obvious step would be to place a notice in the subject line of the message or at the top of the body of the message indicating that this is a privileged work product or trade secret document.

24. To provide additional protection against a claim of having waived privilege, encrypt the message while it is a transmission.[35] On the other hand, I am against encrypting data while it is being stored. In litigation and discovery it may be one year, two years, or five years later that you find you cannot review potentially relevant data files because they were encrypted and you do not know the password. The encryption of stored data can actually create tremendous litigation liability for this reason.

---

33 Also called chat rooms, chat groups allow for real-time interactive conversations between multiple users. *See id.* at 843.

34 Usenet newsgroups are a popular Internet application involving user-sponsored open discussions on a particular topic. Once a message is posted to a group, that message is forwarded to each receiving computer and sorted for a short period of time. Other users with access can then download and respond to the message. *See id.* at 834-35.

35 Encryption involves the use of an equation or algorithm to transfer readable text into unreadable text. *See* Bernstein v. United States Dep't of State, 922 F. Supp. 1426, 1429 (N.D. Cal. 1996).

25. Encryption during transmission, however, may help you preserve privilege. It shows that you have taken additional steps to ensure the privacy of the message. Practical control is built on a well-defined, monitored infrastructure. An example is the carbon copy[36] that is easy to build into an electronic mail system. You can build a group list and use it to send a document to all of the members of that group. Accordingly, it is not uncommon today to find that group, or cc, lists have been built to facilitate mailing to many people. You have to be very careful that you do not click the wrong button and send an important document to the wrong group. Inadvertent distribution is happening with unfortunate frequency in the electronic mail, voicemail, and videomail arenas.

26. The use of the Internet itself can create litigation liability. For example, I know of a products company that set up a homepage and the marketing department conducted a survey to get feedback for product users. They were hoping to build a marketing campaign, using quotes from actual users about the quality of the products. But, do people who love your products write you letters? No. And they are not the ones who respond to Internet surveys either. People were writing back about how the products this company manufactured were doing terrible things. The marketing department realized that they would not be able to build a campaign on such responses. They canceled the survey, but did not tell anyone in the company about the negative feedback. Their own counsel did not know. Soon, there was a product liability lawsuit. The information was found electronically, and was used to show prior knowledge of product defect.

27. What other Internet information can be used against you? Your name, or your company name, is attached to everything that you send out of the organization. Do you want your name attached to everything that is sent out of the organization over the Internet? We have a number of institutional clients whose employees with Internet access have sent strange information out with the name of that institution attached. These employees might have informal, ad-hoc communication with colleagues around the world. They send out information that is later brought back in litigation. The opposing party argues that they have an official correspondence of your organization directly contradicting what you are saying.

28. Libel and harassment issues, and the Communications Decency Act[37] -- cast a new light on Internet use, especially in terms of an organization's obligation to keep information, such as pornography, from being downloaded from the Internet. There is a growing threat of litigation in the harassment arena about data and pictures downloaded from the Internet.[38]

---

36 A carbon copy or "cc" is a duplicate message sent to recipients other than the primary one. *See* WIRED STYLE, *supra* note 2, at 129.

37 Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 133 (1996) (codified at 47 U.S.C. § 223(a)-(h)).

38 *See* Trip Gabriel, *New Issue at Work: On-Line Sex Sites*, N.Y. TIMES, June 27, 1996, at C1.

29. Employees talk about one another and people in other organizations. They carry on conversations and attack people and that comes back in litigation. Copyright issues involving downloaded material are another problem. There are cases where copyrighted material on the Internet has been downloaded into organizations' computer system.[39]

30. The free advice trap occurs when law firms set up homepages and publish legal papers on the Internet. We have one client who is a well-known copyright attorney. He published a number of papers on the Internet and set up a little question and answer section. People would ask him questions and he would offer his advice. He got a call one day from an attorney in another state who said, "Well, you are the attorney for so-and-so, you are the attorney of record." Our client said, "No I am not, I do not even know that person." As it turned out, the person was someone who had asked him a question through the question and answer section. This person came back and said, "I thought you were my attorney. I asked you this question, you gave me an answer that is hurting me now in this litigation, and I am going to sue you." As new technology expands, it is incumbent upon the practitioner to understand the role of that new technology.

31. Another story highlights the role of the practitioner in properly evaluating technology. We had asked a company for some electronic data during discovery. Their attorney said, the information had been deleted. We were skeptical and immediately took a rule (30)(b)(6) deposition[40] of their company's backup administrator. Within 20 minutes of the start of deposition, the supposedly deleted data were found.

32. In reality, the data had not been deleted, but rather had been purged; it had been taken off the live system, put onto a tape, and stored for a year. The information systems person failed to inform the lawyer that purged data could be restored, and the lawyer failed to follow up with questions about the recoverability of purged or deleted data. This oversight cost the company dearly in litigation.

33. The critical point of this story is that you have an obligation and a duty to understand both the terminology and the technology of your client. Your failure to understand these issues will not relieve your clients of their discovery obligations. More and more data is being created, captured, and stored every day. Thousands of people are creating new software platforms. They are thinking up new ways to create, capture, manipulate, and store data. Each time a new piece of software is used within an organization it creates an opportunity or a liability, depending on whether you are the discoveror or the defender.

---

39 *See, e.g.*, Religious Tech. Ctr. v. Netcom On-line Communications Servs., Inc., 907 F. Supp. 1361 (N.D. Cal. 1996) (finding online service not liable when subscriber uploads copyrighted material without authorization and the service provider has taken no affirmative action in the transaction).

40 FED. R. CIV. P. 30(b)(6).

34. The intranet is another popular use of the Internet today. This internal method for communicating raises important issues. It is a huge repository for information. It can have electronic mail and informal chat groups. It can be the central repository where all the information in the organization is downloaded. Outside of the computer group that set up the intranet, users do not know that all the data they download is being stored in the intranet and is available to anybody else on the system. In many cases, access may be available to the entire employee population.

35. Intranet use also creates huge repositories of data. The privilege issue is relevant to the intranet because many times people feel that intranet communication is within the company and that no one else has a right to it. That is obviously not true. Employees will publish material and they will disseminate work product around the company by sending it over the intranet. They think that since it is the intranet, not the Internet, they are somehow protected.

36. The Internet is a world-wide, global network of computers with little or no controls, and no one responsible for management or oversight. This is part of what makes it a very interesting, dynamic environment in discovery. It is a confusing, dangerous, and misunderstood environment. On the other hand, it is also an area that presents the possibility of tremendous productivity for practitioners, attorneys, and students. You cannot ignore it. It has momentum. It is going to be here and it is going to play a large role in shaping communications in this country. It plays a critical role today in research, data acquisition, and in ways people communicate.

37. Huge data transfers are taking place on the Internet and that alone makes it a critical discovery tool. The obligation of the legal practitioner as the Internet grows, changes, and adapts is to be aware of those changes and to ask critical questions such as: Why is this happening? Why are we are adding this new software? What does it do? Does it really delete when you say delete? Do we have the tools to identify, locate, retrieve, and refute data from this system? Do we have the ability within our own organization to handle these tasks?

38. There is going to be a steep learning curve to get up to speed on these issues, but the climb is worth it. That is the direction discovery is taking. Electronic data is already the source of virtually every document you may encounter. There is more paper than ever, but you must not confuse the paper you see with the real source of the paper. The source document is the best evidence. The source document is what you must examine if you want to find out what is actually taking, or took, place. And the source is electronic.

39. Electronic discovery will continue to grow until it becomes the primary source of discovery in this country. All of the information is created, captured, and stored electronically. Electronic discovery is simply a realistic and practical adaption to the real world of information. To fight or ignore it is a dangerous choice.

David Byer:

40. Our next speaker, Judge William Young, has sat on the Federal bench in Massachusetts since 1985. Prior to 1985, he was an Associate Justice of the Massachusetts Superior Court. Judge Young received his A.B. and his L.L.B. from Harvard, and he has been a lecturer in law at Boston University School of Law for many years.

Judge William Young:[41]

41. I will speak briefly about electronic data discovery with specific reference to the court system. I want to tell you three pertinent stories and draw from them a moral. The first story involves a case over which I presided, *Advanced Systems Consultants Ltd. v. Electronic Planning & Management, Inc.*[42] In that case, the gravamen of the complaint was that proprietary data was improperly used by the other side.[43] There was no doubt that the other side had the data; the claim was that they did not misuse it.[44] A witness was called as an expert for the plaintiff. Having examined plaintiff's computer system, the expert found that all the computer files that pertained to the proprietary data had been deleted in the period immediately following service of the complaint.[45] That was extraordinarily powerful information. The defense argued that they were following their normal routine by getting rid of the files.[46] I disagreed and found for the plaintiff for hundreds of thousands of dollars.[47]

42. The second story comes from the criminal trial over which I am now presiding. I have to be very cautious because the trial is ongoing, and I will speak only to things that are public. In the *United States v. Ferber*[48] case, it has been recorded that I have admitted in evidence an e-mail communication. I want to briefly explain what is already in the record. It appears that the defendant, Ferber, made a phone call to an officer of Merrill Lynch. Following the phone call the Merrill Lynch officer wrote an e-mail to his superior at Merrill Lynch. The government has

---

41 The Honorable William G. Young is a United States District Judge on the United States District Court, Court of Massachusetts.

42 No. 94 CV-12522WGY (D. Mass. filed on Dec. 20, 1994).

43 *See* Complaint for Injunctive and Monetary Relief ¶¶ 25-45.

44 *See* Defendants' Answer ¶¶ 20-21.

45 *See Advanced Systems Consultants, Ltd.,* No. 94 CV-12522WGY.

46 *See id.*

47 *See id.*

48 No. 95 CR-10338WGY (D. Mass. filed Oct. 26, 1995).

procured that transmission out of the files of Merrill Lynch. Now think of this as an evidentiary matter. The e-mail is hearsay.[49] The communication is from one Merrill Lynch official to another Merrill Lynch official, so it is not an admission of Ferber.[50] The government claims the communication is inculpatory of the defendant Ferber. How did they get it in evidence? They tried to argue it was a business record, because it is the business of Merrill Lynch, a non-party.[51] I disagreed. They next argued it was an excited utterance[52] because the last sentence was "my mind is mush." But, the very body showed that he had spoken to someone before he sent the e-mail. I did not think that was excited utterance over e-mail. The third basis for admission was a present sense impression.[53] In other words, the statement was made immediately after he had received the communication. It was his testimony that the call had come from Ferber, he thought it was reportable, and he reported it to his superior at the time when someone could have called Ferber back and said, "Do you really mean this?" I allowed it in under the present sense impression exception.[54] Part of that analysis is the temporal business. The e-mail is composed by the speaker immediately and is immediately received electronically by the recipient who is in a position to verify the communication. Whether that is seen as evidence against Ferber I do not know. I can only tell you how I ruled.

43. The third issue in the same case is that the government wants to put in evidence a statement made by Ferber that they will claim is a prior bad act. In order to come in under section 404(b) it has to be the same modus operandi.[55] I ask whether or not he has used these words before. One side says he did; the other side says he did not. As we are in the fourth week of trial, I search my index of words used at the trial to find out if the word has ever been used. It was right there in the database contained in the court's own system.

44. The moral is that within the court systems, especially within the federal courts, we are sitting on a mountain of data. We could have lots of security systems on that data, but we have no right to that. Every time that my colleagues and I

---

49 Hearsay is "a statement, other than the one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." FED. R. EVID. 800(c).

50 *See* FED. R. EVID. 801(d)(2)(A) (hearsay exception allowing admission of a party opponent).

51 *See* FED. R. EVID. 803(6) (hearsay exception for records of a regularly conducted activity).

52 *See* FED. R. EVID. 803(2) (hearsay exception allowing a statement relating to a startling event or condition made while under the stress of the event).

53 *See* FED. R. EVID. 803(1) (hearsay exception allowing a statement describing or explaining an event or condition made while the declarant was perceiving the event or condition).

54 *See Ferber,* No. 95 CR-10338WGY.

55 *See* FED. R. EVID. 404(b) (disallowing evidence of crimes, wrongs, or acts to prove character unless admissible for another purpose such as modus operandi).

make a minute order of one of my chicken-scratching endorsements on the side of the document, that is law. It may be small-time, trial court law, but it is a year and a half ahead of any appellate decision. All the interesting stuff is in the trial courts. There are 13 federal judges in Massachusetts, 72 justices in the Superior Court, and 176 judges of the State District Court, not counting the Probate Court. There is no reason why you should not be able to determine what a particular judge thinks about the law. But, you cannot.

45. If I had an opinion of the Supreme Judicial Court, or the Appeals Court, I would follow it. But I do not have those opinions until a year and a half later. If you gave me the charge of one of my colleagues on the District Court, or if you gave me five or six charges from the Superior Court, I would know the law earlier. That is what those judges think the law really is. Also, every time a person testifies in court, it becomes a matter of public record. You should be able to search the public record and find the testimony. So, although new technology is changing litigation, it may not be in the ways we expect.

David Byer:

46. Our next speaker, Professor Julius Levine, has been a member of the Boston University School of Law faculty since 1969. He graduated from Harvard and Oxford, and he teaches civil procedure and an advanced course in trial advocacy. He has served as Director for the Trial Advocacy program here at Boston University. Furthermore, he has written books on the discovery process and on effective forms of trial advocacy.

Julius Levine:[56]

47. In general, our adversary system began in England without much discovery.[57] There was some discovery in equity[58] and practically none in common law.[59] I think those of us who have gone beyond high school civics realize that the adversary system has some rough edges. One of those rough edges was illustrated poignantly by Samuel Williston in his autobiography.[60] Williston was a fairly new lawyer at the bar and was trying a contract case.[61] He hoped to win as a good

---

56 Julius B. Levine is a Professor at Boston University School of Law.

57 *See* FLEMING JAMES, JR., ET AL., CIVIL PROCEDURE § 5.1 (4th ed. 1992).

58 *See id.*

59 *See id.*

60 SAMUEL WILLISTON, LIFE AND LAW: AN AUTOBIOGRAPHY (1941).

61 *See id.* at 270.

adversary system lawyer. At trial, he produced testimonial and documentary evidence, and rested, waiting for his opponent to present his evidence.[62] They presented some evidence, but he watched and listened very carefully and they never presented a piece of documentary evidence that he had.[63] He thought they probably had a copy of it, but apparently they did not and rested without it.[64] He won the case.[65] However, he says that he felt uncomfortable, because he would have lost the case if they also had the document that was in his briefcase.[66] They did not use discovery and so they lost.[67]

48. Thus, the adversary system went on in its well-known way. But Samuel Williston decided after that experience to change his own career. He became a law professor and wrote treatises on contracts.[68] Although Williston's interest was not discovery, he had been sufficiently impressed in his own career with the very rough edge that appears when discovery is not pursued to have singled it out in his autobiography.

49. So discovery can, when it is done properly and thoroughly by both sides, bring about important benefits in litigation. It brings about evidence that the parties would not otherwise have. In Williston's case, the opponent did not have that crucial document. Discovery diffuses surprise at trial by revealing the information in advance of the trial.[69] Discovery gives both sides the time to think about the information, compare it with other information, follow it up, and expose it as misleading.[70] Finally, discovery helps both parties in their pursuit of evidence to evaluate their cases realistically and, perhaps, have a greater likelihood of reaching a compromise settlement. Therefore, I think discovery is a well-fixed part of our procedural law today and our adversary system is the better for it.

50. When electronic data, computers, and the Internet become widespread and relevant to our discovery law, is there any reason to think that there are differences, mysteries, or surprises in the law? We do not yet have enough cases on this question for a prudent common law lawyer to draw a conclusion. But it does not

---

62 *See id.* at 271.

63 *See id.*

64 *See id.*

65 *See id.*

66 *See id.*

67 *See id.* at 272.

68 SAMUEL WILLISTON, WILLISTON ON CONTRACTS (Richard A. Lord ed., 4th ed. 1990).

69 *See* ROGER S. HAYDOCK & DAVID F. MERR, DISCOVERY PRACTICE § 1.1 (3d ed. 1996).

70 *See id.*

seem so to me, because discovery historically and presently gives parties information about the case. When the information is in a computer, the discovery law should allow the party to obtain it from the computer. California does not have the same rule on discovery of documents[71] as Massachusetts[72] or as applies in federal courts.[73] Since 1970, the federal rule has allowed parties to obtain data compilations from which information can be obtained and translated, if necessary, by the respondent.[74] When the amendment was adopted in 1970, I remember asking colleagues more technologically-oriented than myself what effect it would have on computers. So the rule was ready for us then, and it does not seem to me now that the challenge to the parties or the judge in applying it to some other technology is that significant.

51. I reviewed the First Circuit's recent pronouncement on discovery of electronic data in the *Fennel* case.[75] In that case, a party had to prove when a letter was written. The other party charged that the purported date of the letter was not the real one, but that it had been backdated.[76] In order to prove it was backdated, the expert for the party who wanted to discover testified that he had to examine the hard drive of the word processor that had generated that letter. It seemed to me this was no different than asking under Rule 34 to exhume a time capsule -- to get into a machine and find information stored inside. Rule 34 not only authorizes discovery of documents, but discovery of tangible things.[77] The hard drive is a tangible thing. The expert could find information in there, if not a document. The First Circuit seemed to agree.[78] They did, however, consider the burden to the owner of the computer if its hard drive would be interrupted to an extent that would injure its business. Ultimately, the First Circuit decided the discovery was an undue burden.[79]

---

71 CAL. CIV. PRO. CODE § 2016 (West 1995) (defining a document for discovery purposes as a writing).

72 MASS. R. CIV. P. 26(b)(1) (providing that parties may obtain discovery including books, documents, or other tangible things).

73 FED. R. CIV. P. 26(a) (requiring parties to turn over lists of relevant electronic files and paper documents).

74 FED. R. CIV. P. 34(a) (including data compilations in the scope of discovery).

75 *See* Fennel v. First Step Designs, Ltd., 83 F.3d 526 (1st Cir. 1996).

76 *See id.* at 529.

77 FED. R. CIV. P. 34.

78 *See Fennel*, 83 F.3d at 534.

79 *See id.*

52. E-mail has now have replaced the telephone in many instances. That is a helpful insight for a judge ruling on an objection to discovery of e-mail. Telephone conversations have consistently been discoverable.[80] The most persistent and somewhat successful challenge to discovery has been the list of horribles or abuses that parties practice while undertaking discovery. I am not going to address that topic because I want to have time for questions on today's topic. It does not seem to me that the subject of discovery, the Internet and electronic data, is a more fertile field for abuse than any other. Ever since that criticism first arose in prominent form from the 1950s to the 1960s, studies of the Judicial Conference have admonished that there may be abuses, but have stated that those abuses outweigh the benefits of discovery.[81] Rules 26(c),[82] 26(b)(2),[83] and 26(g)[84] are all in place to curb and prevent abuses and are surely as applicable to the discovery of electronic data as they are to any other information.

53. Justice Powell wrote a footnote in the 1984 case of *Seattle Times Co. v. Reinhardt*[85] that I think summarizes my position as one who has been studying discovery for more than 25 years. He said "abuses of the Rules by litigants, and sometimes the inadequate oversight of discovery by trial courts, do not in any respect lessen the importance of discovery."[86] It is very important for us to sleep better than Williston was able to sleep after his opponent failed to use discovery. We will do that if we are not shy in employing discovery to obtain materials off the Internet and other electronic media.

David Byer:

54. Our final speaker is Don Leka. Don is the corporate counsel for Teradyne, Inc., a manufacturer of automatic test equipment in Boston. Prior to joining

---

80 *See* Union Const. Co. v. Western Tel. Co., 163 Cal. 298, 305 (1912) (noting discoveries and inventions that have become of common and general use); Theisen v. Detroit Taxicab & Transfer Co., 200 Mich. 136, 136-39 (1918) (addressing admissibility of telephone conversations).

81 *See* COMM. ON RULES OF PRACTICE & PROCEDURE, JUDICIAL CONFERENCE OF THE UNITED STATES, LOCAL RULES REGULATING ATTORNEY CONDUCT 3 (1995).

82 FED. R. CIV. P. 26(c) (providing authority for the court to grant protective orders).

83 FED. R. CIV. P. 26(b)(2) (allowing the court to limit discovery if too burdensome or duplicative).

84 FED. R. CIV. P. 26(g) (granting the court authority to impose sanctions for improper discovery).

85 467 U.S. 20 (1984).

86 *Id.* at 35 n.20.

Teradyne, Don worked at Hutchins, Wheeler and Ditmar and then spent seven years as counsel with The Gillette Company. Don graduated from Yale and Harvard.

Don Leka:[87]

55. The remarks that I will make this afternoon, to the extent that they are intelligible at all, are not to be considered the policies and practices of Teradyne, or any other listed company. I will begin with a controversial proposition, and that is to suggest to you that businessmen are people too. I will not try to defend that, but I would ask you to accept it for the moment as an operating assumption. What this proposition means is that businessmen come in all shapes and sizes, degrees of intellectual prowess, and levels of ethical responsibility. The real point is that they have a different perspective on the purpose of the organization. I would suggest to you that lawyers describe their organization as striving to minimize or eliminate exposure to risk. They try to place their organization in the best possible position for litigation. Businessmen will say they want to market widgets and sell them for profit. The point is that as lawyers make a number of suggestions, programs, and proposals about the Internet and electronic discovery, they may be greeted with a degree of skepticism.

56. I offer some examples. For any company that has a records management program[88] -- although what we really need to call it is a records destruction program[89] -- we need clearly, articulated policies that are published and understood by all employees. We want to make sure we have some teeth in this records management program. If we do not show that there are teeth in this program, when the time comes for discovery the lack of a policy will be a factor in determining documents still exist. The businessman may say, "I have a pack rat in my organization who is my chief design engineer. He is the one that keeps the flow of projects coming in. Are you telling me that I should give him instructions that his job is in jeopardy unless he cleans out the computer files over six years old, even though when litigation happens it will require an archaeological expedition of his office? I, as a businessman, will take that risk rather than impose some rules that are going to stifle what he is trying to do within our organization."

57. As any lawyer who practices in that field will tell you, the purpose of an environmental audit is to protect the results from examination by government agencies or litigators. Therefore, you must note that the requests come from the legal department so that it will not create a problem if there is an investigation. In

---

87 Donald Leka is Corporate Counsel at Teradyne, Inc.

88 *See* Karen S. Guarino, *Developing A Comprehensive Records Management Plan*, 7 HEALTH LAW. 15, 15 (1994).

89 *See id.* at 16.

the meantime, we will lobby for legislative protection against this information being made available to anyone else. Then the businessman will say he wants to get out there and get the information on what processes need improvement. And in order to make that work, the information must be disseminated widely and discussed, rather than filtered through the legal department. The rebuttal by the lawyer will typically be that we must guard against the possibility that drafts, preliminary thoughts, or careless statements which might be misconstrued by unfriendly eyes, should be discovered. The surrebuttal by the businessman can be unflattering, "You mean to tell me that because the truth might theoretically come out some day, maybe in a messy way, I should make it harder to do the job against real problems today?"

58. The basic conflict is that the lawyer defines the goal of the organization as removing or minimizing legal liability, while the businessman defines the goal as making widgets and selling them at a profit. When the businessman disagrees with the lawyer, ignores legal advice, or fails to implement every recommendation, these acts are not defying the law. The acts arise from a different perspective on the nature of risk and its relative importance in the overall scheme of things.

59. My point is that lawyers should have sensitivity to the opportunity cost of their recommendations. How disruptive are they? How concrete are the benefits obtained or the risks avoided? I do not mean you always settle for less than optimum. That is true sometimes, but at other times it is just a matter of how you package or present the recommendations. The topic of Internet security fits within this pattern. Here it can be shown that there is no real conflict with business goals and legal objectives. When the information services groups create firewalls for the Internet or password protocols for e-mail, input from a lawyer will be useful.

Question and Answer Session

Audience Member:

60. It has been common wisdom, at least until recently, that for a lawyer to communicate confidential information or advice over the Internet and through e-mail is foolhardy because such action risks compromise of confidential client information that may result in liability on the part of the lawyer and waiver of attorney-client privileges. Is the Internet as secure as the telephone? Should we use it for communication of confidential information, and should lawyers feel free to communicate confidential information over the Internet with as much security and confidence as they do over the telephone? Any comments on this controversy?

John Jessen:

61. Communications being sent over the Internet and virtually all other communications systems have the potential of being intercepted. Is it a risk that there are people watching the Internet for specific information? I believe the Internet is not a secure environment for the transfer of information unless additional steps are taken to secure it. I do use the Internet for communication. However, I would not use a cellular telephone for communicating confidential information, because there are tools and methodologies to grab that information out of the air. I am not advocating not using the Internet because I think we need to use it. There are tremendous productivity issues involved. You should, however, use it in such a way that you gain the productivity without sacrificing your client's privilege.

Judge William Young:

62. I do not know the technology, but if the parties communicate in such circumstances must they reasonably protect themselves against disclosure to other parties? The law has not developed to the extent that we can know what reasonable protection is for e-mail. The law also says that if you take steps to reasonably protect yourself, and you are overheard inadvertently, tough luck.[90] That is not so now. Indeed, there are a few cases that apply what is, in essence, suppression similar to a criminal trial where the other side got the communication, but the disclosure was inadvertent and therefore the court suppressed it.[91] The reason I think those cases were wrongly decided is it puts the party claiming the privilege in a better position, because the party that inadvertently got the communication has to show that their discovery was free of the inadvertent. The key question seems to be: Were reasonable steps taken to make the communication secure? If they were, I do not think it is crystal clear that by using the Internet you waive the privilege. On the other hand, the Internet is an insecure medium.

63. The Wiretap Law[92] was amended in 1986 to include electronic mail. E-mail systems in 1986 looked nothing like they do today. But there are two systems, open and closed. Closed systems are corporate systems used by employees. That does not imply safety because there is no privacy right for e-mail under that corporate system. An open system, such as a provider of e-mail services, does have more of the privacy protections against interception. Intercepting commercial, open-system e-mail is a felony punishable by a $10,000 fine.[93] The Wiretap Law does not

---

90 *See* Pereira v. United States, 374 U.S. 1, 4 (1954).

91 *See, e.g.,* People v. Moss, 583 N.Y.S.2d 699, 701 (N.Y. App. Div. 1992) (suppressing statement made to defendant's brother in hospital but overheard by a police officer).

92 18 U.S.C. § 2511 (1994).

93 *Id.* § 2511(4).

accurately address the different privacy rights that courts grant open and closed systems.

Audience Member:

64. I have a question touching on what Mr. Leka said about a destruction policy, and what Professor Levine said about potential proof. One thing that I have come across, being a junior associate, is the sheer magnitude of discoverable material and mandatory federal disclosure requirements. What obligation does a law firm have and how should I help shape the client's document retention policy in looking at things covering a particular time frame? Does one search 1,000 employee e-mails on a daily basis over a year? How do you come to grips with your advisory obligation in a cost efficient manner?

John Jessen:

65. At the moment, I have about 150 cases involving electronic data discovery. It is very difficult for an organization to identify, locate, retrieve, and review all possible electronic data if they have not addressed the issue in advance. You must begin to incorporate data management and retention issues in to your work with your clients if you are going to fulfill your role as counselor. The more prepared an organization is to identify, locate, retrieve, and review electronic data in a discovery event, the better you are going to look.

Julius Levine:

66. In the 1980s and 1990s, the rules on discovery were amended to add a basis for the court to rule that discovery should be limited based on the party's resources, the amount in controversy, and the importance of the issues at stake in the litigation.[94] If you have a mind boggling volume of paper that is larger than you had before computers, and the case does not justify the expense, you invoke rule 26(b)(2).[95] Maybe by invoking the rule, both sides might agree to limit the discovery and each reveal the key information. So there is room for creative compromise in carrying out the provisions of the rules. I think parties should not be bashful in bringing these questions to court early to get satisfactory resolution there. You cannot conduct litigation that costs you more resources than you have saved.

---

94 FED. R. CIV. P. 26(b)(2) (allowing a court to limit discovery if burden outweighs benefit).

95 *Id.*

John Jessen:

67. We are seeing an increased use of special masters to determine what is a reasonable production. An independent, third party is often useful in placing limits on the amount of electronic data to be reviewed and in determining how and when data will be shared.

Judge William Young:

68. Data discovery is a profound question and it is practical to address it at the start of a lawsuit. It is at this time that you learn what questions to ask of your client. Today, in litigation, you must invest in discovery immediately, and the client must marshal resources either for attack or defense. If the client is not prepared to do that, it is time to buy out the lawsuit. That is the biggest change in the economics of litigation, especially in the federal courts. It used to be that you invested a lump sum of money to complain, answer, and move to dismiss, and then you dribbled out the money in a gradually escalating litigation budget until you were spending much money on the eve of trial and pre-trial. Wrong. Lawyers find it difficult as an economic matter to get over it. The change is money up front; more money than the corporate people expect to pay in every case. If you do not want to do it, settle the case. We call it cost and delay reduction. But you are most affected at the beginning because this is like gas warfare. No one really knows the cost-benefit analysis. So negotiate early on.

69. How do you organize your files so that you can search them and isolate information that would not be privileged? It is magic to me, but imagine advising a client to organize their files in a particular way so as to minimize the costs of responding to litigation demands.

Don Leka:

70. I would like to put the earliest disclosure in federal cases into the context of the law in unintended consequences. Another example is the federal statute to limit the size and frequency of federal class action securities litigation.[96] The securities laws may create more litigation because now they have a certain type of safe harbor[97] -- if you do not happen to say the right safe harbor words, you will find yourself in litigation that you would not have been in before. I also suggest to you that in federal cases when there is an obligation to show to the other side the important documents in your case, you will tend to turn over everything and try to

---

96 *See* Private Securities Litigation Reform Act of 1995, Pub. L. No. 104-67, § 27, 109 Stat. 737, 738-749 (1995) (codified at 15 U.S.C. §§ 77a-78).

97 *See* § 27A, 109 Stat. at 749-56 (1995) (providing a safe harbor for meaningful cautionary forward-looking statements).

create an avalanche. Otherwise, there will be a dispute some months down the road that this set of documents that you did not turn over is important.

Audience Member:

71. What if the other side turns around and gives me everything demanded? What is the magnitude of effort in terms of what I need to do? Do I have to hire some kind of outside expert? What are the costs?

John Jessen:

72. We rarely see organizations choosing to dump data on the other side. Most likely, you are going to get a selected response to your requests. Even those limited responses, however, may pose huge processing problems for you. If you are going to ask for electronic data, you should have a plan as to how you are going to deal with the data when you get it. You need to consider your ability to quickly and economically process different kinds of data on different kinds of electronic media such as tape, diskette, and hard drive. If you do not have the in-house ability to process large volumes of disparate data on varying media platforms properly, you should seek outside assistance.

Audience Member:

73. What are the implications of telecommuting and working at home?

John Jessen:

74. Home use computing is an interesting issue. I was in Manhattan two weeks ago in the general counsel's office of a very large company when the president of that company walked in and said to the counsel, "Sometime today I would like you to explain to me why last night during dinner two sheriff's deputies and a lawyer came to my home and seized my home computer." He then turned around very calmly and walked out. The national counsel for this company who had been working there for many years was fired because they had not advised the company on proper steps to avoid ex parte discovery orders from being entered against home computers. If home computers are being used for corporate work, they are going to be fair game in a discovery proceeding. You must consider this line of discovery when you are pursuing data, and you must remember this when advising clients on possible areas of liability.