UIC John Marshall Journal of Information Technology & Privacy Law

Volume 25
Issue 4 *Journal of Computer & Information Law - Symposium*

Article 3

2008

Litigating at the Boundaries, 25 J. Marshall J. Computer & Info. L. 609 (2008)

Keith G. Chval

LITIGATING AT THE BOUNDARIES

KEITH G. CHVAL*

No doubt, the intersection of information, technology, and litigation is an exciting place to be operating. It is truly is amazing point in time in terms of the confluence of developments in these three venues, and it's been a lot of fun for me personally. I left the Illinois Attorney General's office about two and a half years ago to work at Protek International with my partner, an F.B.I. veteran of twenty-eight years. We have about two and a half years worth of experience at these crossroads in terms of the investigative, computer forensics, and eDiscovery perspective. I have also had the benefit of being a participant in events at this intersection through my work as a litigator. It has been tremendously interesting to witness, and be a part of, this rapidly developing area of the legal landscape.

My proposition to you here today is, the confluence of developments in these three areas: information, technology, and litigation, has conspired to create a veritable perfect storm in terms of its impact on each. Today, I will be focusing primarily upon the impacts as they relate to litigation. There are several factors that have contributed to creating this perfect storm scenario in terms of the impacts on litigation. One of them is the fact that computers are everywhere. Second, they capture all kinds of information, some of it you might expect to be retained in computers, or what we call computers, but some you might be quite surprised to find out is actually also there. Finally, the last and maybe most critical element, is that lawyers are starting to get it, which just adds an extra element that, when it hits litigation, makes things very interesting.

Computers truly are everywhere. Take a look, here's just a quick sampling of some of the things that maybe you would have, or would not

* Keith Chval is the co-founder of Protek International, Inc., a practicing attorney with the law firm of Connolly, Ekl & Williams P.C., where he leads the firm's technology-related practice area, and an adjunct professor at The John Marshall Law School. Mr. Chval conceptualized, created, and supervised one of the nation's pioneering high tech crime units at the Illinois Attorney General's Office. Mr. Chval's courses at John Marshall include information technology, privacy law, economic espionage, cyber crime, electronic discovery, digital evidence, computer forensics, and information warfare. He has a J.D. from IIT Chicago Kent College of Law and a B.S. from Indiana University.

have, thought of as being computers. You go from the gazillion of different sizes and shapes of thumb drives, they are in watches, they are in this, they are in that. Thumb drives everywhere now hold about thirty-two or sixty-four gigabytes. A thirty-two gigabyte thumb drive that you just plug into the USB drive. In a mainstream audience, not too many have nearly that much. Basically, on a thumb drive you could easily copy everything of any value or interest from your computer. As another example, consider the surveillance cameras that are everywhere, or, for that matter, any kind of camera now.

At first blush, you may not have thought of these devices as computers, but many jurisdictions have very expansive definitions of what constitutes a computer. For example, under Illinois law, a computer is defined something to the effect of anything that can process, store, retrieve, or transmit data. So that is the "computer"; almost everything is on a computer these days. In essence, I would defy you to think of a place, or some area of your life, that there is not a computer or a computer has not touched on it. Virtually from your microwave, to your thermostat, computers are everywhere.

Second, they capture all kinds of information. There is the expected, as it is intended in the workplace, in business, in corporations and in education, everything has gone electronic. Ninety-nine point nine percent of corporate documents are created or stored electronically. At Protek, we are in a suite near to a couple of law firms. One of the lawyers had his college-age daughter working during the summer and she needed to use the typewriter. She looks at it and says, "How do you turn it on?" What do you use a typewriter for anymore? Virtually everything is created and stored electronically today.

Less than a third of all electronic documents are ever printed. So they do not even make it to hard copy. An estimated one hundred eighty-three billion e-mails were sent each day in 2006. So all those Bill Gates smoking-gun memos are just floating around out there -one hundred eighty-three billion opportunities to pick-up on something of that nature. Sixty percent of business critical e-mail information, remains contained within corporate e-mail systems. These facts are just a playground for litigators to go looking for valuable evidence for their case.

Then there is the unexpected information captured by these "computers." Sure we expect our computer systems to retain documents and e-mails and all that kind of stuff; that is what they are supposed to do. But the way some of those devices work, the way Windows works, or different operating systems work, they end up retaining a whole lot of information that maybe you would not have expected.

We get regular calls in a trade secret or proprietary information kind of environment where an employee has left and –the former em-

ployer is afraid they have done XYZ or taken whatever proprietary list with them. One of the initial ways we will begin our inquiry is by asking,

> "Do you have USB drives on your computers? Did you have a policy about the use of thumb drives or not?"
>
> "No."
>
> "Did you ever see the person carrying a thumb drive?"
>
> "Well, yes we know he had a thumb drive."

So, we'll start taking a look, and one of the things that the system maintains or retains is information about files that were accessed off a thumb drive. So, we can now in many instances say, "Yep, based on that file path of this recently accessed file on the system, it points back to a file on the thumb drive." So here on a thumb drive is a document entitled Sales Brochure.pdf perhaps that might be relevant to the new employers. Packaging.pst, Product Brochure.pdf, and the list goes on and on of documents that somehow made it to a thumb drive that the person had. Now the other thing that we can find about thumb drives often is a unique identifying number, a serial number for a thumb drive. So if we can pull that out of the system, sometimes the new employer did not know what was going on, that the person was bringing a bunch of stuff with him, or at least they did not want to know about it. The old employer's attorneys will contact the new employer and say,

> "You know you've hired this guy from us; he was a very important person. He had access to x, y and z, and we're concerned he's brought. . ."
>
> "No, no, no, he wouldn't do that."
>
> "Well how about if we let our forensics guys come over and take a look at your computer and see if the serial number for that particular thumb drive that was on our system made it to your system?"

Nice way to kind of tie the ends together, but again something that the majority of people would not expect, that level of information to be retained within those computers.

Consider digital cameras, metadata associated with digital cameras is called EXIF data and here is the kinds of information retained there. The data includes: the brand of the camera, the model number and the date and time stamp of when it was taken. So, if we are trying to say, put it back in that person's hands, we will say, "Let's take a look at that camera you got there and see if the serial number matches up to what we found associated with that picture."

Many of the manufacturers are now putting GPS information in them which would be a wonderful for vacation pictures ten years later when you are looking at your pictures trying to figure out where they are from. If you have the GPS coordinates, you can imagine the uses for it in litigation if you can now tie that picture to where it was taken. These are things that you might not expect, cameras and cell phones all have

GPS in them, all kinds of possibilities like that. You have to think for a minute about what might be there either associated with a file, or associated with a system that file was located on at one point or another.

Another example are the black boxes, event data recorders, in vehicles. A lot of people are aware that those exist, at least on most cars, but you start looking at the kind of information that is available with those and most would be quite surprised: vehicle speed, engine speed, throttle position, brake status, seat belt status -the list goes on and on about the data that it collects for that vehicle at a given point in time. Obviously this is evidence that could be critical in related litigation.

Take that application even one step further, and how many would think that marine engines would also have event data recorders that record key information related to warranty coverage such as whether you exceeded the maximum rpm's within the initial break-in period. So, a friend of mine's engine blew during that period and he took it back to the marina where he bought it from and said, "Hey, my engines blown I want it repaired or replaced." The owner said, "Well, hang on just a second." He retrieves what is some sort of an event recorder from that engine and, fortunately for my friend, the rpm's were within the warranty standards. But that is the kind of information available in places you never probably would have expected, at least until you start thinking about it a little bit.

The last piece contributing to this perfect storm is that lawyers are starting to get it. I guess the question you might ask is, "Why that's just happening now when computers have been around for quite a while and Al Gore invented the Internet back in '94 or so?" Why is this finally happening now after lying dormant for so long? I would point to the presence of two of the classic motivators that are now present: pain avoidance and pursuit of pleasure.

First, Ken Withers, who's now at the Sedona Conference, was quoted in an article from a couple of years ago. "Ninety percent of the information is in the electronic form and they're only asking for eight percent of the information, if you're only asking for hard copies of documents. Obviously they're not getting a full picture of what's going on." Okay, well that's nice to hear but the punch line of that is the subsequent observation from the article that they're potentially exposing themselves to malpractice because they're not adequately seeking in discovery what could be there or might help their client.

To bear out his prediction, the Morgan Stanley lawsuit from a while ago back in 2005.[1] Kirkland & Ellis, and not to cast any aspersions on anybody one way or the other, was representing Morgan Stanley, and it is just a whole fiasco about how the e-mails were disclosed after an inordinate amount of time and what the court considered to be less-than-

1. Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co. Inc., No. SC07-1251, 2007 Fla. WL 4336316 (Fla. Dec. 12, 2007).

forthcoming representations to the court. On the eve of trial, Morgan Stanley whose general counsel was formerly about a thirty-year partner at Kirkland & Ellis, fired Kirkland & Ellis and indicated in their court filings that they were considering a malpractice action against Kirkland & Ellis.

So first, obviously the desire to avoid the pain of a malpractice lawsuit would be a significant motivator for most attorneys. Second, there is the bad press and the effect that it might have, having that kind of thing out there in the newspaper that you allegedly bungled a case to this degree. The language that the court used was equally as harsh as what Morgan Stanley was saying at the time about how the attorneys handled things. I think there is a lot of additional context that could be added to that, which might tend to paint Kirkland and Ellis in a different light. Maybe it was not all Kirkland & Ellis' fault so much as it was some of the challenges of understanding technology and IT operations as well as the dynamics of client relations. But obviously, attorneys are starting to notice these kinds of things, saying, "We better get a handle on this stuff and start handling our e-discovery and our electronic information more closely, or we're the ones who are going to be in the headlines, or worse."

Then take a look at each of these digital headlines from the past several years to get a sense of the reward out there for being aware of the possibilities that electronic evidence may play in litigation and pursuing the pleasure that harnessing that electronic evidence can mean for your litigation. If you look at these prominent cases over the years where some form of digital evidence played a critical role in pushing that litigation, that prosecution in one direction or the other, either it was the smoking gun that put the nail in the coffin, or it was the exculpatory thing that said, "that's not what it looks like, here's what really happened here, this evidence is contrived." But in all those cases for which you just saw the headlines, and a whole bunch more that you regularly see in the news, the electronic evidence has played a key role in which way that litigation or prosecution went.

Obviously as a lawyer, there is little more satisfying than winning that case, and a close second to that would have to be seeing the new clients walking through the door because of your successes. So, the reward is clearly there, and attorneys are aware of all the valuable evidence, or at least becoming more aware, of all that valuable evidence that might be electronically stored on a computer.

So rather than the question mark after whether it is a perfect storm or not, I think it is safe to say that it is in fact a perfect storm, and I will point to three major areas of impact where we have seen it play out.

First, is obtaining that electronic evidence through what we are now calling "electronic discovery." Second, is in terms of how the evidence is

being most effectively, persuasively, used in court. Finally, getting rid of the evidence, or to put it more euphemistically, the great enterprise effort to effectively manage their electronically stored information, or ESI, so as to reduce the number of digital haystacks through which they must search for potentially responsive ESO and to also have a better handle on where the ESI that they have retained is actually located.

It used to be that there was a certain Texas gentlemen's agreement when it came to how attorneys dealt with ESI in discovery. "You don't ask for my electronic evidence, I won't ask for yours, we'll all be happy, it's a huge headache to deal with this stuff, forget it." But all you need is one wise guy in the mix to say, "Yeah, you know what, as a matter of fact, I do want your stuff." The *Zubulake* case which is a well known case within the eDiscovery ranks is kind of the prototypical case for blowing away the Texas gentlemen's agreement environment. It represents a David and Goliath-type scenario where you have a lone plaintiff pursuing a much larger defendant – typical in certain employment litigation scenarios. There, the employee is a lone entity, typically without a whole lot of electronic records that can be discovered so, they are in a great position to say, "You know what UBS? I want all your e-mails from anybody that had anything to do with anybody that talked about this case and I want you to preserve all your ESI, and make sure you dig through all of the back-up tapes too while you are at it." Can you imagine what they have to go through to get all that evidence? To identify where it may be, preserve and collect it all, restore it from archives, to process, review and analyze it all? But what can they demand of her in return? "Okay, but you're going to have to do the same with all of your ESI?" "All right fine, here's my one computer, here's my one external whatever." So, that Texas gentlemen's agreement first started to breakdown where either an attorney who recognized and was willing to act on this disparity in the volume of potentially responsive ESI, or where an attorney who knew what they were doing with regard to electronic evidence and said, "I'm not afraid to defend it. I'm not afraid of a request made of me; I want your stuff." Well, there are still vestiges of the Texas gentlemen's agreement, but it broke down pretty much to where it was more like the Hatfield's and McCoy's. Attorneys were fighting about electronic evidence up and down and up and down. They were fighting about what is available or not. "I think there's an e-mail out there that you didn't get and I want that one." "My client saw a memo once, or an e-mail once, and I swear it's somewhere in your system so I want my forensic guys to come and inspect your system." Can you imagine the disruption it causes their systems?

Recognizing that things were devolving to the point that greater energy was starting to be spent litigating the eDiscovery issues rather than

the substantive issues in a case, the now famous 2006 amendments to the Federal Rules of Civil Procedure were promulgated.

The rule changes touched upon several areas relating to the discovery of electronic evidence. First, we now have a new acronym to throw around. You have probably all seen by now over and over again the term ESI, or electronically stored information. We do not call it computer data or whatever else; it is electronically stored information, ESI. And you know what? Its discoverable! As odd as that may seem, it was not that long ago that you would have a response to a discovery request where the other side would say that it is in a computer, it is never been printed out, therefore it is not discoverable; it does not exist because it is in a computer. That argument is actually memorialized in at least one written opinion. It was a loser. But just to make sure we are all clear about it now, the Rules changes make it clear that, first of all, we are going to call it ESI and second, it is discoverable! Many observers suggest that the changes really are not that revolutionary from what was already taking shape through case law. However, I think most would agree that perhaps one of the most significant impacts of the Rule changes is that it put eDiscovery at the forefront.

Up until the changes, sometimes attorneys would kind of lie in the weeds with regard to ESI issues and then jump on their opponent for his failure to preserve some obscure piece of ESI well into the litigation when it is too late for them to preserve something that was in existence before. The rules push it out front with the meet and confer conference to discuss, among other things, the realm of electronic discovery. Attorneys are asking these questions sooner:

> What documents are you going to want? How do you want to get them? Do you want them in native? How do you want them produced? What if any metadata are you interested in? Do I need to preserve unallocated space? What about tape backups? How much is it going to cost to do that? If you have a reason why you say you can't do it, then I want to hear about it now.

We want these things discussed up front so we are not playing a game of "gotcha" somewhere down the line. That is having a big impact on things and people are getting smarter about it and realizing, "Okay the gig is up; I can't hide my stuff anymore. I can't claim that I can't retrieve my ESI anymore." I would like to be able to tell you that there has been this universal effect where everyone now gets it and we are no longer hearing some of the nonsensical arguments for why they cannot produce their ESI, but it is not quite so.

I just received a call last night from an attorney, and it is one of these situations where two individuals are suing a major financial services corporation and they are looking for e-mails. The response back was: "We can't do that." There's an affidavit on file, and I don't know if I

laughed or cried when I saw it last night, but there's a response on file , "We can't do it because it's in archive and therefore we can't; to get out of archive is just so hard to do. Then once we do that we have to search it manually because we cannot run search terms by subject line or by text or receiver and sender." I'm just thinking, "Are you kidding me? How can you say this?" Then they say, "Well, it would be too burdensome because we've got so much litigation going on right now that it would be somewhere in the queue and it would take us forever to get to." I am thinking that if you have all that litigation going on that you are doing this already, you are probably pretty good at retrieving your e-mails and searching them and culling them down with tools rather than manually. But this is going on today, and from a major firm - which apparently missed the headlines about how they are getting hit with sanctions for spoliation and other issues because they are actually trying to refuse to produce those e-mails. So, the rules only take us so far but they are getting us in the right direction. The battles continue.

The second impact or element of this perfect storm is with regard to the admissibility and persuasive use of digital evidence in court. It is one thing going through the discovery process to get the electronically stored information. The next thing then is how it plays out in court. There is a two-part component to that. One is just simply admissibility, and again it is another one of those things where for a long time people just said, "Well it's a business, if it's an electronically stored record, it's a business records, it's an exception, it's not hearsay." They would call someone to the stand to pass as the keeper of the records if the opposing party really makes them, they go through kind of the same old rote business records exception foundation and we are off and running. Well it is starting be that it's not quite a given that, if you do that, you are going to get your business records ESI admitted.

In *American Express v. Vinhnee*, a bankruptcy case, there was a situation where American Express had a default judgment against an individual and were moving to prove it. The defendant was not present at the time that the judge said, "You know I don't think you laid the foundation for those electronic records." They had somebody there that was in the IT department that came in and said, "Yeah, these are our records from our system, we keep them in the ordinary course of business, etc. etc." The judge responded,

> But you don't say anything about how those computers worked or what software was being used on them, whether it was reliable, etc. I'm not going to let those records in but I'll tell you what, I'll give you a chance to supplement your record, you can submit in writing how you would lay the foundation for that and I'll take that into consideration.

Well, American Express did that, and the court still said, "Sorry, you didn't do a good enough job." They were awarded substantially below the

judgment they were seeking. Just to kind of rub salt in their wounds the court said, "On those other two claims, had you produced sufficient evidence of the foundation, you would have prevailed on those too." So it is not necessarily such a given anymore that if you just produce somebody whose kind of familiar with the computers and systems that your ESI is going to be admitted.

So, admissibility is becoming a greater hurdle to cross with regard to electronic evidence. In response to that there is one working group at The Sedona Conference right now with regard to these general issues that is working on standards in terms of the Federal Rules of Evidence for admissibility of electronic evidence. They are trying to figure out how you standardize it so that predictability is there, so we know what it is going to take to lay the foundation and get it into evidence. So that is the next thing that we are going to see coming out of Sedona, and whether it eventually makes it to be an actual Amendment we will see.

The second aspect of how this perfect storm is impacting ESI in the courtroom is how attorneys are going about maximizing the persuasive value of their ESI. I do not know how many here have had the joy of hearing, after you lay a foundation, you argue back and forth with the other side about whether you have laid sufficient foundation and the judge finally says, "I'll let it in for what it's worth." Or, "I'll let it in and I'll give it its proper weight." Well, if you are the proponent, you are in trouble because the judge has basically just told you that she is tired of hearing about it, does not want to argue about it anymore, but she is not going to look at it as a persuasive piece of evidence.

So, the next piece that is playing out there that attorneys are getting an understanding of is the persuasive use of ESI. From the opponent's perspective, if they can just create some kind of cloud of doubt around the evidence, even if it comes in, the judge or the jury is going to think, "I don't understand what it means about EXIF data from a Cannon X34 who says that works? Forget it, I'm done." So the second part is how to build up the persuasiveness of this piece of evidence that was admitted into evidence. That is kind of the two-part thing as far as how it is playing out in the court system.

Finally, the third impact. Do you remember Carnivore? It was the FBI's alleged e-mail monitoring and communication monitoring system. It supposedly caught everything that ever crossed the wires. It was highly controversial in terms of the potential infringement upon privacy and civil rights. And what did the FBI call it? Carnivore! Well, when it comes to this third impact, the efforts of enterprises to get a handle on the enormous volumes of stored data that they are accumulating, at least the people that are dealing with this stuff are smart enough to call it "document retention" when really the point of the whole exercise is document destruction. Because a lot of what this is about is that we do not

want to keep more electronically stored information than we have to. All that does is drive up storage costs, and more importantly, creates huge headaches for us when called upon to identify, preserve, collect, search, and review it in the discovery process.

So, we are going to talk about electronic records management and document retention, what we are going to keep, not so much about the ESI that we are destroying through that process. The other part that is playing out now and creating a lot of opportunities for lawyers and other people to work with companies and entities to figure out that they should empty their e-mail inbox every once in a while. "Could you clear out the deleted files? Can we archive what we really need to archive and clear out the rest?" You do not need to have every version of that memo that ever existed. Assuming that litigation is not pending, let us have policies that require us to regularly purge the stuff out so when we do get litigation we do not have to go through two yottabytes of data looking for two or three files or e-mails. We have got it narrowed down. By the way, if it happens that there was no litigation at the time, and it happens that that smoking gun that Bill Gates had written way back when was innocently destroyed pursuant to an established document retention program well, that is just kind of a side benefit too.

That is another benefit of reasoned document management retention policies and procedures. They also help to protect from spoliation claims. There is a wide range of duties under which an enterprise is required to maintain and preserve ESI. There are all kinds of regulatory requirements, whether it is in healthcare or the financial services, whatever else. There are certain records that are required to be kept. And once litigation is a possibility, there are certain records you are required to keep. So, if you do a good job of applying reasonable document management and retention policies and procedures, and litigation holds, in those scenarios, then you are protecting yourself from the other side claiming spoliation, and even if you did inadvertently destroy something you can say, "We did the best we could. We had reasonable measures in place, this is what we did, we had a policy, we followed it and you know something did get screwed up. But we did the best we could." That goes a long way with the court. Those are three of the more significant impacts of this perfect storm that has been created by the confluence of information, technology, and litigation.

To this audience, I am probably preaching to the choir to say that my charge to you would be to embrace your inner geek, at least when it comes to litigation anyways. Tap into the broad universe of digital evidence that's out there, and use it to your advantage. If you are not a geek, find a geek you can embrace and use him or her to help you harness the power that is there in that digital evidence, and to protect you when others are throwing their digital evidence at you.