2014

Symposium on the Challenges of Electronic Evidence

Daniel C. Capra

Sidney A. Fitzwater

Peter Pitegoff

Jeffrey S. Suttom

Paul Grimm

See next page for additional authors

Repository Citation

Capra, Daniel C.; Fitzwater, Sidney A.; Pitegoff, Peter; Suttom, Jeffrey S.; Grimm, Paul; Haried, John; Bruegge, Richard W. Vorder; Bellin, Jeffrey; Scechtman, Paul; Smith, Deirdre M.; Scheindlin, Shira A.; Shonka, David; Gelb, Daniel; Goldsmith, Andrew; Paul, George; and Lippe, Paul, "Symposium on the Challenges of Electronic Evidence" (2014). Faculty Publications. 1833.
http://scholarship.law.wm.edu/facpubs/1833

Copyright c 2014 by the authors. This article is brought to you by the William & Mary Law School Scholarship Repository.
http://scholarship.law.wm.edu/facpubs
THE PHILIP D. REED LECTURE SERIES

ADVISORY COMMITTEE ON EVIDENCE RULES

PANEL DISCUSSION

SYMPOSIUM ON THE CHALLENGES OF ELECTRONIC EVIDENCE*

MODERATOR

Prof. Daniel J. Capra, Reporter

CHAIR

Hon. Sidney A. Fitzwater

PANELISTS

Peter Pitegoff, Dean
Hon. Jeffrey S. Sutton
Hon. Paul Grimm
Hon. John A. Woodcock, Jr.
Gregory P. Joseph, Esq.
John Haried, Esq.
Richard W. Vorder Bruegge, FBI
Prof. Jeffrey Bellin
Paul Shechtman, Esq.
Prof. Deirdre M. Smith
Hon. Shira A. Scheindlin
David Shonka, Esq.
Daniel Gelb, Esq.
Andrew Goldsmith, Esq.
George Paul, Esq.
Paul Lippe, Esq.

* This Panel Discussion was held on April 4, 2014, at University of Maine School of Law. This transcript of the Panel Discussion has been lightly edited and represents the panelists’ individual views only, and in no way reflects those of their affiliated firms, organizations, law schools, or the judiciary.
I. OPENING REMARKS

JUDGE FITZWATER: Good morning, everyone. On behalf of Judge Jeffrey S. Sutton, and the members of the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States, my colleagues on the Advisory Committee on Evidence Rules, and our Committee Reporter, Professor Dan Capra, welcome to the Symposium on the Challenges of Electronic Evidence.

We are indebted to the University of Maine School of Law for its willingness to host this symposium, not once, but twice, because we were scheduled to hold the symposium last October before the government shutdown caused it to be cancelled. I want to particularly thank Dean Peter Pitegoff and Professor Deirdre M. Smith for making the symposium possible and for the warm welcome our committee has received. I also want to thank our colleague on the Evidence Committee, Chief Judge John A. Woodcock of the District of Maine for his gracious hand in ensuring a successful symposium and meeting of the Evidence Rules Committee.

This is the third in a series of symposia that the Evidence Rules Committee has convened. In 2011, we held a symposium at the William & Mary Marshall-Wythe College of Law on the then-newly-adopted Restyled Rules of Evidence.

The underlying purposes of that symposium included enhancing understanding of the restyled rules by exploring the painstaking process by which they were formulated and identifying evidence rules issues that remain to be resolved even after restyling.

In 2012, we convened a symposium at the Charleston School of Law, devoted to a single rule of evidence—Rule 502, a Rule of Evidence adopted by Act of Congress at the request of the Judicial Conference of the United States—to discuss ways in which that rule could be better known and understood so that it could fulfill its original, salutary purposes.

At today’s symposium, we are proceeding from that more narrow examination of one Rule of Evidence to a considerably broader conversation about a subject that is as wide-ranging and seemingly limitless as the digital world of today. We are considering the challenges that electronic evidence poses to the Rules of Evidence.

In a real sense, we are asking ourselves whether rules that have been thoughtfully developed over time—some over a very long period of time—to ensure that every proceeding is administered fairly, without unjustifiable expense and delay, to ascertain the truth and secure a just determination, have continuing vitality when measured against how people speak, act, and think in an electronic world.

We are fortunate indeed to have drawn again from the best and the brightest to participate as panelists in this symposium. They represent a truly distinguished group of judges, lawyers, and scholars.

As I have said of our prior panelists, they are distinguished, not merely because they are accomplished individuals, but because they have expertise and extensive experience addressing the issues that appear to be most
pertinent to the bench, to the bar, and the academy—indeed, to the purposes for convening this symposium.

By convening this symposium—and by arranging for these proceedings to be added to the legal literature through publication in the *Fordham Law Review*—the Advisory Committee on Evidence Rules is attempting to anticipate and address proactively technological changes that seem almost certain to increase in speed and complexity.

To paraphrase Winston Churchill, this is not the end of this process. It is not even the beginning of the end. But it is, perhaps, the end of the beginning.

We are fortunate to have assembled a group of noted judges, practitioners, and academicians to assist in this worthy goal. I welcome you all to this Symposium on the Challenges of Electronic Evidence.

And we are fortunate to have with us today one of our hosts, Dean Peter Pitegoff. Dean.

DEAN PITEGOFF: Thank you, Judge Fitzwater, and thank you all for coming. I’m Dean of the University of Maine School of Law. And on behalf of the law school, let me say how pleased we are to host the annual meeting of the Advisory Committee on Evidence Rules and the Symposium on the Challenges of Electronic Evidence.

We’re particularly honored to welcome such a distinguished group of judges, lawyers, and scholars, as Judge Fitzwater said.

And I’d like to give a personal thanks to Judge John Woodcock, Chief Judge of the U.S. District Court here in Maine, for arranging to hold this meeting at the University of Maine School of Law. University of Maine School of Law is the public law school of Maine, the only law school of Maine. And we take seriously our mission to serve the public and to promote justice in Maine and beyond. This event today resonates so well with that mission, bringing expert voices to Maine from throughout the nation.

I’d like to give further thanks, of course, to Professor Dan Capra, Fordham University School of Law, as the organizer of the symposium.

And to my Maine Law colleague, Professor Deirdre Smith of the University of Maine School of Law, for her participation in the symposium and for representing the law school in the planning process.

I look forward to a robust discussion of very, very timely and pressing issues today. And again, welcome.

II. INTRODUCTION OF THE PANELISTS

PROFESSOR CAPRA: Thank you, Dean. I’m Dan Capra. I’m going to be the moderator today. So the first order of business is to introduce the panelists. And I’m going in alphabetical order. Jeff Bellin is an associate professor at William & Mary Law School, where he teaches evidence, criminal procedure, and related seminars. He clerked for Judge Garland, U.S. Court of Appeals for the D.C. Circuit, served as a prosecutor with the

And he is, I think it’s fair to state, the foremost scholar on the topic of electronic evidence. His article on “Present Sense Impressions” impressed Judge Fitzwater to such an extent that he decided it would be a good idea to hold this conference.

Daniel Gelb is a partner at Gelb & Gelb LLP in Boston. He represents clients in general and white collar criminal defense matters, complex civil litigation, and arbitrations. And prior to joining Gelb & Gelb, he was an ADA for the Norfolk County District Attorney’s Office in Massachusetts. He’s a frequent speaker and author on electronic discovery. And he works closely with the Sedona Conference.

Andrew Goldsmith is the Justice Department’s National Criminal Discovery Coordinator. In this role, he oversees a wide range of national initiatives designed to provide federal prosecutors with training and resources related to criminal discovery, including electronic discovery. He’s published a number of articles in the area.

We are very lucky to have Paul Grimm on our panel. Judge Paul Grimm serves as the District Judge for the United States District Court for the District of Maryland. He’s a member of the Advisory Committee for the Federal Rules of Civil Procedure, chairs the Advisory Committee’s Discovery Subcommittee, which means he is a busy man these days.

His opinions on electronic discovery and electronic evidence have been widely influential. And he teaches courses on evidence and discovery at University of Baltimore School of Law and University of Maryland School of Law.

John Haried is the Criminal Discovery Coordinator for the Executive Office of United States Attorneys in the Department of Justice, where he coordinates discovery policy and training for the Department’s United States Attorneys. And he’s helped develop the New Recommendations for ESI Discovery in federal criminal cases. He frequently lectures on e-discovery, electronic information management, and the privacy of electronic communications.

Greg Joseph is a past president of both the American College of Trial Lawyers and the ABA Section of Litigation. He was a charter member of the Advisory Committee on Evidence back in 1993 when it got reconstituted pursuant to Judge Becker’s article and direction.

We are honored to have two charter members of the committee sitting right here, Greg and Ken Broun.

Greg was cochair of the Third Circuit Task Force on Selection of Class Counsel. He’s the president of the U.S. Supreme Court Historical Society, and a founder of Joseph Hage Aaronson, a law firm with offices in New York and London. And he’s the author of Modern Visual Evidence.

Paul Lippe is CEO of OnRamp Systems, the leader in legal department platforms to improve quality and efficiency and reduce costs of legal work. He was at various times general counsel and senior vice president, business development and corporate marketing at Synopsys, an electronic design automation company.

Also, Paul was CEO of Stanford SKOLAR, a medical digital library. And he speaks regularly about the new normal in law. He will be our closing speaker today.

George Paul is an experienced business litigator and partner in the Litigation Practice Group at Lewis & Roca in Phoenix. He’s a recognized authority on digital evidence. He authored the ABA’s book, Foundations of Digital Evidence,3 and coauthored The Discovery Revolution.4 He’s the author of a number of articles on electronic discovery and electronic evidence5 and co-chair of the ABA’s Electronic Discovery and Digital Evidence Committee.

Shira Scheindlin is a United States District Judge for the Southern District of New York where she’s served since 1994. She previously worked as an AUSA, commercial lawyer, Magistrate Judge in the Eastern District, and is known for, among other things, her landmark opinions on electronic discovery, the Zubulake6 and Pension Committee7 opinions.

She was a member of the Advisory Committee on Civil Rules from 1998 to 2005 and a coauthor of the first casebook on electronic discovery and digital evidence.8

JUDGE SCHEINDLIN: With Professor Capra.

PROFESSOR CAPRA: Paul Shechtman began his law career as a law clerk to Judge Louis Pollak and then clerked for Chief Justice Warren Burger.

Paul served as AUSA, and then became Associate Professor at the University of Pennsylvania School of Law. Eventually, he became Chief of the Criminal Division of the U.S. Attorney’s Office for the Southern District of New York.

And he’s now in private practice at Zuckerman Spaeder. He has taught evidence and criminal procedure for twenty-five years now at Columbia

Law School and is a member of the Judicial Conference Advisory Committee on Evidence Rules.

David Shonka is the Principal Deputy General Counsel at the FTC. He oversees the Office of the General Counsel’s Litigation, Legal Counsel, and Opinions and Analysis groups, he is a member of the Sedona Conference, he serves on the steering committee for the working group on e-discovery and electronic records, and frequently speaks on these topics. And it’s old home week here because he graduated from the University of Maine School of Law.

Deirdre Smith is Professor of Law and Director of the Cumberland Legal Aid Clinic at the University of Maine School of Law where she teaches evidence and mental disability law and supervises student attorneys in the clinical program. Her research focuses primarily on the intersection of psychiatry, mental illness, and evidence law in the context of civil litigation. She’s chair of the Maine Supreme Court’s Advisory Committee on the Rules of Evidence.

Jeffrey Sutton, who will be our introductory speaker, is a judge on the United States Court of Appeals for the Sixth Circuit. He was formerly a partner at Jones, Day, Reavis & Pogue in Columbus, served as State Solicitor General for the State of Ohio, served as a law clerk for Justices Powell and Scalia on the Supreme Court, and to Judge Meskill on the Second Circuit.

And he is the Chair of the Judicial Conference Advisory Committee on Rules of Practice and Procedure and, as such, is the boss of all of us today, the way I look at it.

Richard Vorder Bruegge is the senior photographic technologist at the FBI, where he is responsible for overseeing science and technology developments in imaging science. He’s got a Ph.D. in geology from Brown University, and has worked at the FBI, where he’s performed forensic analysis of image and video evidence and testifies in many courts as an expert.

And we’re thankful to have him here. And I want to thank Betsy Shapiro of the Justice Department for lining him up because the projects he’s working on are very timely and relevant for what we’re going to be doing here today.

And finally, John Woodcock, Chief Judge of the United States District Court of the District of Maine. Before his appointment to the court, Judge Woodcock practiced law in Bangor and served as an ADA. He is a member of the Advisory Committee on the Federal Rules of Evidence. And he’s also a member of the Subcommittee of the Standing Committee on CM/ECF and its effect on the Rules. He’s spoken widely on the effect of technology on the courts and the state and Federal Rules of Evidence. And he received his J.D. from the University of Maine.

And so I would like to turn it over to Judge Sutton.
III. THE CHALLENGES OF RULEMAKING ON QUESTIONS OF TECHNOLOGY

JUDGE SUTTON: I want to thank the Dean and the University of Maine School of Law, as Sid said, for inviting us not once but twice. Thank you. And to Sid and Dan, thanks for your leadership on this great symposium.

I just want to make three basic points about technology in the practice of American law. I hope to start things off and to give a little bit of a sense of what the Standing Committee and the different subject matter committees are doing, not just related to evidence, but actually, more related to some other subject matter committees.

It’s pretty difficult to deny that technology is changing the way American law works. Discovery is an example. The volume, the expense of producing discovery in American litigation has changed exponentially because of e-discovery, because of electronically stored information (ESI).

Perhaps just as significant are the preservation obligations because there’s nothing more terrifying to a plaintiff or a defendant than the possibility of sanctions for destroying evidence once litigation has started.

This happens to be an area where not just the expense but the risk applies to plaintiffs and defendants. Yes, defendants in big corporations have to worry about lots of people who have iPads and iPhones and all kinds of servers where you have to preserve this information. But the obligations now put the plaintiff at risk too.

Think of the single-plaintiff employment action where someone files a lawsuit against their employer for employment discrimination. Three months after the lawsuit, they change their Facebook page, they get rid of their iPhone. They potentially destroy evidence. Should the same rules apply, or should we have different rules that apply there?

E-filing is basically universal. I read all my briefs now on an iPad. I don’t print them out anymore. By the way, it makes it very hard to read footnotes. So do not use footnotes, if I were you, which is all for the good, as far as I’m concerned.

Filing deadlines have basically disappeared. It’s now midnight instead of 5:00 p.m. It’s the day of. It’s 24/7. I sometimes wonder who the master and who the servant is in this whole situation. We think of technology as serving us, but I’m wondering more and more if we’re now the slaves as opposed to the masters of it.

We have to monitor jurors because now they have access to everything. And we need to be worried about whether they’re going to check out a Wikipedia page and confirm something.

And if I worry about jurors, I worry even more about judges, particularly Court of Appeals Judges who want to take judicial notice of everything. Judge Posner was recently doing experiments in his office as to how quickly one could don and doff clothing for work.

And, you know, Wikipedia is out there. Judge Kozinski gave a talk the other day where he said in the Google litigation, they denied a motion based
on information they found online where they tried to check whether something was actually damaging anybody.

And I think it’s not just that we have to keep up with technology, I think technology is changing norms.

A wonderful example of this is privacy norms. If any of you have children, you know that, with Facebook, texting, chat, whatever these things they’re doing, I don’t think they believe in privacy. I think privacy is another word for loneliness. And I don’t think they want to have anything to do with it. So privacy norms are changing because of technology.

So what do we do? There are three ways in which law can respond to change. One is Congress. The Constitution makes it very difficult for divided government to accomplish anything. And in that sense, the Constitution is working perfectly. So that’s not a perfect solution in terms of changing law to account for technology, although it works sometimes.

Then there’s court decision-making. And court decision-making is often the way we do this. It has the risk, however, of often being under-inclusive and over-inclusive in addressing problems.

I think some people that are critics of the Supreme Court summary judgment decisions in the mid-1970s, as well as more recently in *Iqbal* and *Twombly*, would say those were over-inclusive overreactions to perceived problems in American litigation, many of which grew out of American discovery problems and the costs of litigation.

That leaves the third option—you might not be surprised to hear it’s my preferred option—and that’s the Rules Enabling Act process. And that’s amending rules to account for changes in technology.

The Rules Enabling Act process does have one conspicuous flaw, although I think it can be a benefit in the long haul, and that’s that it’s very slow. If you have a brilliant idea today, the fastest it can become a new rule is three years.

It has to go through the Advisory Committee, in this case the Evidence Committee, then the Standing Committee, then the Judicial Conference, and then the Court. And then Congress can’t do anything for six months.

So it is slow. And with technology, that’s a little scary because the fear is you start down a road in 2010, say, which is what the Civil Rules Committee has been doing, to try to deal with civil discovery reform. And by the time you make changes in the current rules you’re hoping will go into effect at the end of 2015, technology has changed and maybe altered the nature of the problem.

So it’s not a perfect process because it’s so deliberative. But it is also inclusive. And because we can gather data and get all kinds of experts through symposia like this, I think it does work very effectively.

So I thought I’d just give you a couple of things that the Rules Committees are working on and then start these panels. The Civil Rules

Committee, as Judge Grimm well knows, has been working since 2010, since the Duke conference, to really engage in discovery reform.

And the basic themes have been more cooperation among lawyers and more proportionality in discovery so that not everything that’s relevant is necessarily discoverable. There has to be some proportionality between what’s being sought and the expense of what’s being sought given the stakes of the litigation.

As for the preservation obligations, we’re trying to make sure that Civil Rule 37 makes sense in an ESI world. So we’re right in the throes of that, and we’ll know in the next few months what that’s going to look like. I know Judge Scheindlin is going to talk a little bit about a Rule 37 proposal today.

The other thing we’re doing is accounting for all of the rules and how they need to change with the onset of universal electronic filing. Take something like the three-day rule. Does that rule make sense when people are automatically served? Well, I would say not exactly. Should we be so focused on font size and the color of a brief when I haven’t seen a blue or a red brief in a long time? Not exactly. So maybe all that has to be adjusted.

Electronic signatures are another problem. In bankruptcy, most things are done electronically. That’s increasingly true for other filings. Well, that’s a potential problem for fraud. And so how do we figure that out? The U.S. Department of Justice is very interested in coming up with a solution that works there.

Then last but not least is, of course, the evidence rules. And that’s exactly what we’re doing today. And thanks for being here. And I can’t wait to hear what you have to say. And we’ll try to make it law within three to five years. Thank you, Dan.

PROFESSOR CAPRA: So the way today will proceed is we’ll go through several topics that present issues in terms of challenges of electronic evidence.

And I just wanted to set up just for a quick second where we are at least, the Evidence Rules Committee, in terms of electronic information.

The Committee has been concerned about electronic evidence for a number of years. More than ten years ago I started looking, at the direction of the Chair and Committee, into concerns about the fact that the Rules of Evidence at that time largely didn’t speak in terms of electronic evidence.

There was a reference to “data compilations” in the business records exception to the hearsay rule. But, for example, there were hearsay exceptions that referred to books and publications. Basically, it was a paper-based set of rules.

No action at that time was taken, because it was determined that the courts were dealing with those rules, using them to admit electronic evidence basically on the same principles they would admit hard copy.

12. See Fed. R. Civ. P. 6(d) (allowing three extra days for electronic service). The Civil Rules Committee has proposed an amendment to delete this time period.
So, for example, there’s a case in the Second Circuit where a learned treatise was offered, but as a video. And the opponent took the position that a video is not covered by the learned treatise exception because the exception only refers to publications in books and treatises. And Judge McLaughlin wrote a wonderful opinion about how Rule 101 of the Federal Rules of Evidence is intended for breadth and to reach a fair and just result, so why would we exclude it simply because it was in electronic form? Courts were generally applying that kind of flexible approach to electronic evidence.

The restyling effort, however, gave the Committee a chance to update the language of the rules, to accommodate electronic evidence without actually changing any substantive rulings of the courts. And the way that was done was by amending Rule 101 to add a definition that any reference to a writing also includes similar information in electronic form.

That language at least basically modernizes all of the rules by way of definition. And believe me, talking to the other reporters in the other committees, it’s a good thing to have. They want that rule. That’s to update their own rules, which are also paper-based.

But what the restyling did not solve was whether, even if the rules do cover electronic information by word, the basic evidentiary concepts need to be retooled to deal with electronic information. And that’s what we’re going to discuss today.

IV. AUTHENTICITY

PROFESSOR CAPRA: I think we start with authenticity because, at least as far as I can see, that is the major issue among courts and litigants about how to deal with electronic evidence. As to authenticity if it’s a hard copy, you can fairly easily see whether it’s been altered. If it’s electronic, it’s more difficult. And the question is whether that possibility of alteration should result in any different standard of authenticity. Another question is whether electronic information can be managed and retrieved in such a way as to permit easier methods of authentication.

And we’re thrilled to have people who know so much about authenticity here today. We’re going to start with Judge Grimm.

JUDGE GRIMM: Good morning, everyone. And thank you all very much for the warm hospitality and welcome.

I recently finished a two-and-a-half week sex trafficking trial where the evidence included evidence of social media sites, licit and illicit. A lot of digital video evidence. It included location evidence that was connected in with cell phone location, and text messages and iMessages, which are distinct, although they look the same on your phone.

14. Id. at 170.
15. Id. at 170–71.
There were issues involving authentication, hearsay, issues about everything except the original writing rule. I’m thinking of writing an article about the original writing rule. If you’ll recall, the original writing rule, forgotten, but not gone.

And it was a reminder that today with the explosion of digital media, and everything that involves how people interact is going to come into our courts, and we’re going to be faced with dealing with this evidence.

My responsibility in the few minutes that I have allotted to me today is to give an overview of the evidence rule that has seemed to be the most challenging for the courts; that’s authenticity. The basic rule, 901(a), establishes the requirement of authenticity or identification for nontestimonial evidence.

Rule 901(b) gives ten illustrative nonexclusive examples of how you can authenticate. Rule 902, which is self-authentication, is another tool available as well, but doesn’t come up so much with digital evidence.

Rules 104(a) and 104(b), however, are very important rules, which are rules that when you read them in the rule book, you say to yourself, “How in the world would I apply these? If I ever tripped over these rules in a dark courtroom, would I know how to use them?”

And with authentication of digital evidence, you can have a question about what’s the judge’s job versus the jury’s job if there is a reasonable dispute of fact and a fact-finder could find that the evidence either is authentic or is not.

The beginning place is Rule 901(a). “To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.”

This is a reminder of my misspent youth. I grew up at a time when parents would on Friday evenings go to an event that was referred to as a cocktail party. And they would come home in a fashion that my father would refer to as tired and confused.

And we children were told do not interrupt until they emerge in a nontired and nonconfused fashion tomorrow morning. And that meant that we would get up early in the morning on Saturday. We’d go down to the kitchen. We would get a bowl that was filled with some sort of product that was composed mostly of sugar. We would pour in large amounts of milk that had as much fat as they would hold. Buttermilk, preferably. And then we would watch cartoons until the parents emerged from the cave.

And one of the cartoons that we watched was “Popeye the Sailor Man.” I have no idea why we did when I look back now. But if you recall, and don’t admit it if you do, that Popeye’s mantra was “I am what I am.” And that is authenticity. You only have to show that the evidence “am what it am.” And that is a very low threshold, preponderance, more likely than not.

17. For Judge Grimm’s PowerPoint presentation, see Appendix I.
So how do you show with digital evidence that it “am what it am?” Rule 901(b) has ten methods, some of which are more wired to evidence associated with corporeal or three-dimensional evidence.

So, for example, Rule 901(b)(2) provides for a showing of authenticity by a witness’s familiarity with handwriting. And I suppose I’ve signed enough things at the supermarket with my little wand with my signature that that could be familiarity based upon digital handwriting. But typically, it’s handwriting in a tangible fashion.

But one of the authentication tools most likely to be encountered in authenticating electronic evidence would be Rule 901(b)(1), a witness with personal knowledge. That’s the email I sent. That’s the email I received. That’s my email address. This is my Twitter post. And that’s the type of evidence that is pretty straightforward. Rule 901(b)(3) is an interesting authentication method where the fact-finder can look at a known exemplar, known authenticity, compare it with an unknown example and be their own expert as to whether it’s the same. Or you can bring in an expert to compare a known and unknown. And I suppose our FBI examiner here can tell us about how that function is done every day in courtrooms by people with expertise.

Rule 901(b)(4) is a utility player in this area. 901(b)(4) and 901(b)(9), the next two, are perhaps the most useful in this process because 901(b)(4) provides for authenticity based on distinctive characteristics or circumstances. It looks like a duck, it walks like a duck, it quacks like a duck. It must be a duck.

And so if you get an email from Paul@gmail.com, and it’s signed Paul. And I use all those little annoying emoticons, the colon and the parentheses and whatever else to show—and I’m known to do that. And I have a very good friend, Judge Mal Mannion, who is as Irish as they come, and he always sends emails in green ink. And there are aspects about my communications that are unique to me. Then through circumstantial, inferential reasoning, you can say more likely than not an email from Paul@gmail.com that talks about things that Paul knows about, responding to something that Joe sent to Paul, is authentic because it was by Paul.

And then finally, Rule 901(b)(9): when all else fails, bring in the experts, and establish a system or process capable of producing reliable and accurate results.

---

19. Id. 901(b)(2) (providing an example “of evidence that satisfies the requirement” of authenticity: “A nonexpert’s opinion that handwriting is genuine, based on a familiarity with it that was not acquired for the current litigation”).
20. “Testimony that an item is what it is claimed to be.” Id. 901(b)(1).
21. “A comparison with an authenticated specimen by an expert witness or the trier of fact.” Id. 901(b)(3).
22. “The appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances.” Id. 901(b)(4).
23. “Evidence describing a process or system and showing that it produces an accurate result.” Id. 901(b)(9).
Now, my role is not to talk about hearsay, but there are some interesting issues coming up now where you have computers that generate what may be referred to as assertive statements that are offered for their truth, but they’re done through a scientific process.

There is no human declarant under Rule 801(b), so they can’t be hearsay; but yet they come in because a process has been designed to do an analysis and give a result, like a drug test. And that implicates then a system or process. So oftentimes, what may appear to be a hearsay issue is, in fact, an authentication issue. So that’s the framework.

Now, what about Rules 104(a) and 104(b)? Rule 104(a) requires the trial judge to make a preliminary evidentiary determination regarding three things: (1) the admissibility of evidence, which is all the foundational determinations; (2) the qualification of witnesses, so that would be for experts and whether someone is competent; and (3) the existence of privilege.\textsuperscript{24}

And when the judge does that preliminarily, before it goes to the jury, that’s the gatekeeper rule, the Rules of Evidence with the exception of privilege are inapplicable. Which means that affidavits and hearsay, all those types of tools, can be used to determine whether or not the evidence is admissible, and authenticity is one of those examples.

So the notion of Rule 104(a) is very prominent, and that’s what Rule 104(a) is. The Rules of Evidence do not apply. There is an analogue that is found in Rule 1101(d)(1), providing that the facts upon which the judge relies to make a determination under 104(a) are not bound by the Rules of Evidence except for privilege.\textsuperscript{25}

So you can use leading questions, you can have affidavits, you can use hearsay for the purpose of the judge making that threshold determination.

But let me pose the hypothetical that has really gotten a lot of the state courts on a confusing cycle that has not fully been played out yet.

Let us imagine that—you have to realize that evidence comes in on a continuum. There is an offer. If it is clearly authentic, there’s no objection. It comes in.

There’s an offer. There’s an objection that it’s not authentic. You turn to the lawyer and say, “What’s the evidence to authenticate?” They lay the foundation. You turn to the lawyer for the other side and say, “Do you have evidence contrary to that?” “No, I don’t. They just haven’t met their foundation.” The judge then decides if it comes in.

But now suppose that you have evidence that shows that it was authentic, that is, it was a website. It was prepared by a person with their name, with their picture. It’s got characteristics that tie it to them. But now you have

\textsuperscript{24} “The court must decide any preliminary question about whether a witness is qualified, a privilege exists, or evidence is admissible. In so deciding, the court is not bound by evidence rules, except those on privilege.” \textit{Id.} 104(a).

\textsuperscript{25} “These rules—except for those on privilege—do not apply to the following: (1) the court’s determination, under Rule 104(a), on a preliminary question of fact governing admissibility . . . .” \textit{Id.} 1101(d).
evidence that someone else has been posting things on their website or on their social media site without their permission.

And the issue is: did this particular person, whose state of mind is relevant, post it or not? And we have competing versions. Yes, they did. No, they didn’t. What does the judge do then?

If the judge makes a preliminary determination that a reasonable jury could find that it is authentic, but also, a reasonable jury could find that it is not authentic, then the trial judge does not make the final call on admissibility.

This implicates perhaps the most enigmatic rule in the Rules of Evidence, 104(b), which is conditional relevance: that when the relevance of evidence turns upon the establishment of a fact, it is admissible subject to the proof of that fact or conditionally upon its establishment.26

But if there is a dispute of fact that it is relevant only if authored by the defendant, and there’s a legitimate dispute about whether the defendant authored it, until the fact-finder charged with resolving fact issues weighs in on that, then you cannot determine ultimate relevance.

In that particular instance, the trial judge’s function is to preliminarily determine whether or not the threshold showings for authenticity and nonauthenticity have been made, and then to give it to the jury with the instruction: “Ladies and gentlemen of the jury, you have heard evidence that this email was authored by the defendant, and you have heard evidence that it was not. If you find more likely than not that it was authored by the defendant, you may consider it and give it the weight that you believe it is entitled to. But if not, you must disregard it and give it no weight whatsoever.”

Then the jury, when it deliberates, goes, and you don’t really know until the end when you get the verdict. You triangulate about whether the jury accepted it or didn’t accept it.

That is—the difference between Rules 104(a) and 104(b) is uniquely found with digital evidence where there is this fear that is constantly being discussed in the media and in decisions about people being able to hack or to set up a fictitious website or a fictitious social media site.

Or we’ve all had the situation where someone borrows our phone. My daughter says: “Oh, Dad, I need to send a text to my friend, can I use your phone?” I hand my phone to my daughter. She sends a text message.

So all of these notions are very, very, very pervasive to us. Technology changes constantly. And one of the great fictions of our life is—two fictions, as our first speaker, Judge Sutton, said, that there is no such thing as privacy.

So we have a fiction that there’s privacy, but the other fiction is that our technological devices that we use in our lives are more or less secure for the purposes for which we use them. That is a fiction because if we realized

---

26. “When the relevance of evidence depends on whether a fact exists, proof must be introduced sufficient to support a finding that the fact does exist. The court may admit the proposed evidence on the condition that the proof be introduced later.” Id. 104(b).
realistically, we would all curl up in a fetal position in our rooms and never come out.

So this notion of Rule 104(b) is particularly important when we deal with issues of digital authenticity.

And finishing up, let me just alert you to where the battlefield is playing out. Now, I’ve got to tell you upfront, candor requires me to give you a disclaimer.

There are two schools of thought working their way through the courts, the state courts today. One of them is approached by my own state, Maryland. And that was in *Griffin v. State*.27

In that court opinion, with a MySpace page that communicated a threat, the Maryland Court of Appeals held that the proponent of digital media evidence had to negate the possibility that there was fabrication of the evidence as part of the basic foundation for authenticity, despite the fact that there was no evidence introduced to show that it was not authentic and all of the circumstances connected it with the defendant’s girlfriend.28

That’s the one approach, and it is very strict.

The contrasting approach in Texas29 and in Delaware30 [is] that if there is evidence that it is authentic that a reasonable jury could find, and there is evidence that it’s not authentic, it becomes a Rule 104(b) issue. The jury gets it with an instruction from the court.

But if there is only a specter that someone may have spoofed it or have fabricated it, that is not a sufficient challenge if the proponent has shown authenticity by a preponderance.

And these two courses are going in opposite directions. I will tell you that all three have cited an opinion that I authored in 2007, *Lorraine v. Markel American Insurance Co.*,31 which means it’s a totally useless opinion because it can be cited for diametrically opposite conclusions on the same issue.

So for that reason, this is the notion of what authenticity is. I think my time is up. And I’m happy to participate in any discussion.

PROFESSOR CAPRA: I did have one question, Paul. Since *Lorraine* has screwed everything up at the federal level, is there something for the evidence rules to do to actually deal with exactly the situation you’re talking about?

JUDGE GRIMM: I don’t think so. I think the rules do it magnificently. I just think candidly the distinction between Rules 104(a) and 104(b) is absolutely an enigma to most people, to most lawyers, and to most judges.

A lot of judges are—trial judges are phenomenal in terms of the gut versus the head. They know with a gut-level feeling, is this enough for it to go to the jury or not. And that part about authenticity they get.

---

27. 19 A.3d 415 (Md. 2011).
28.  Id. at 423–28.
Usually what will happen, and in these decisions, with the exception of *Lorraine*, I have never seen an opinion that actually talks about Rule 104(b) and fits it with Rule 104(a).

They’ll talk about Rule 104(a), and they’ll talk about the jury deciding the weight, but that’s a Rule 104(e) weight versus admissibility distinction.\(^{32}\)

PROFESSOR CAPRA: My reading of the federal cases is they take essentially the Texas, Delaware, more permissive approach fairly uniformly. That approach is more consistent with the low threshold of admissibility for questions of authenticity established by Rule 901(a).

JUDGE GRIMM: Absolutely. So this is not a tinker-with-the-rule issue. This is perhaps the absolute personification of our inherent uncertainty and feeling a little bit ill at ease with all of this technology. We use it. We don’t know how it works. We hope it works OK. But we’re sort of worried behind our mind that it doesn’t, but we can’t help it anyway because we can’t live our lives without it.

PROFESSOR CAPRA: I’d like to turn it over to Judge Woodcock.

JUDGE WOODCOCK: I’m going to start with the proposition that the Rules of Evidence can be broadly divided into two categories. The first category is rules that are rules based on how people act. And the second category is rules that are based on what people make.

For rules that are based on how people act, the rules are largely immutable. I suspect that Iago’s statement, “I hate the Moor,”\(^ {33}\) was a statement against interest in Shakespeare’s time and will always be that.

Rules that allow or disallow the admissibility of the things people make, however, are based on the technology that underlies the object. And unlike human nature that underlies what people do, the technology that underlies what people make is constantly changing.

The challenge of the rules is to test the premise of admissibility against the changes of technology to make certain that the reasons for admissibility remain valid.

To explain my concern, I’ll start with a further subdivision between the things that normal people make and the things that lawyers, as opposed to normal people, make; the familiar but hazy line between admissible evidence and demonstrative evidence. And with the rubric that the best way to analyze a digital piece of evidence is to reduce it conceptually to paper, to start with what you know is real and work from there.

To give an example, I’ll start with a photograph. Our rules contemplate that once the foundational witness has identified the content of the photograph as depicting accurately what it purports to depict, to use Judge Grimm’s “I am what I am,” and I would add, “and that’s all that I am,” the photograph is allowed to go into evidence. And it is allowed to be taken into the jury room for use during deliberations.

---

32. “This rule does not limit a party’s right to introduce before the jury evidence that is relevant to the weight or credibility of other evidence.” FED. R. EVID. 104(e).

33. WILLIAM SHAKESPEARE, OTHELLO act 1, sc. 3.
I suggest that the admissibility of that photograph is bottomed on our implicit understanding about the technology of the photograph. That the modern photograph under our sense is a more technologically sophisticated daguerreotype created by light bouncing off an object and returning to a plate of silver or copper.

For evidentiary purposes, it is proof, often convincing proof, that the photographed object is or was what is shown in the photograph.

And it is particularly powerful evidence. Jurors looking at a photograph and comparing it to the contrary testimony of a witness would likely have the same reaction as Groucho Marx: “Who are you going to believe, me or your own lying eyes?”

At this point, I’ll shift to the Margaret Chase Smith Courthouse in Bangor where I preside.

Over the jury box is a professional photograph of Judge Gene Carter. Judge Carter is dressed in a robe, looks highly distinguished, against a background of a shelf of law books. Except that—and I know this only because he told me—the actual photograph was taken in front of a fireplace. And the books were photoshopped into the photographic portrait.

How would the Carter photograph be received into evidence? If a lawsuit centered on where Judge Carter was when the photo was taken, and a witness were willing to testify he were in front of a [fireplace], who would the jury believe, the lying photograph or the truthful witness? If altered, is the Carter photograph admissible or is it demonstrative evidence?

The Carter photograph issue presents itself in innumerable ways. Is the scandalous photograph of the employee from her or someone else’s Facebook page an accurate image of what happened or has it been manipulated? Is the computer-generated hotel registration log an accurate reflection of what a handwritten log would look like or has it been altered?

The list goes on, and in today’s trial, questions of accuracy affect nearly every piece of technological evidence. In federal court, we are often presented with cases where someone’s life, liberty, or fortune is on the line. Is there any doubt where the stakes are so high that if evidence can be easily manipulated, it will be? Is there a gap between what jurors assume they are seeing—namely, old, difficult-to-manipulate technology—and what they are actually seeing, namely, easy-to-alter technology?

In other words, are jurors, consciously or not, following the analytic rubric and reducing the photograph to the equivalent of paper when they are, in fact, dealing with ones and twos variously displayed to form what looks like a photograph, but is not?

Is there a generational divide on the issue? Is the new computer-savvy generation so skeptical about the accuracy of computer-generated images, documents and the like, that they are jaded when they should not be, discounting the truthful photograph in favor of a lying witness?

The questions I pose include: Should the Rules of Evidence begin to reflect differences in technology, underlying different types of exhibits? Should an old-fashioned photograph be easier to admit than a digital image? Should a digital image be admissible purely on the say-so of Popeye?
If not, by what standards should the admissibility of the new technology be judged? Should trial judges caution jurors about admitted images, computer printouts, and other digitally created evidence and their potential limitations? Should the Rules of Evidence allow for an investigation into how the potentially admissible digital objects were created so that the images can be reverse-engineered to determine their authenticity?

Are we, in effect, creating a body of evidence that would be subject to a future Innocence Project demonstrating that evidence underlying convictions was manipulated or false?34

I will end with a story by Daniel Boorstin, the great American thinker, who in the 1960s wrote a book called *The Image*, which first addressed the difference between reality and images.35

He told the story of the proud mother approached by an admiring woman who says, “What a beautiful baby.” And the mother responds, “That’s nothing. You should see her photograph.”

The question I’m raising is whether the difference between the baby and the image should cause us concern when a lawyer moves into evidence the digitally created image as exhibit one.

PROFESSOR CAPRA: Thank you, Judge. So do we need to have detailed rules on foundation for digital photographs in the Federal Rules of Evidence?

JUDGE WOODCOCK: I’m going to follow up with what Judge Grimm said—I think it’s more an issue of discovery. I think that’s where the rubber is meeting the road here.

PROFESSOR CAPRA: For civil cases. For criminal cases as well?

JUDGE WOODCOCK: I think so. Yes.

JUDGE SCHEINDLIN: Professor, could I ask a quick question?

PROFESSOR CAPRA: Yes.

JUDGE SCHEINDLIN: My question as a trial judge to you is: If the adversary doesn’t challenge this at all, am I supposed to do this on my own and say: “Well, tell me more about this photograph. Where was it taken? Who took it?” How do I know? Or leave it alone? Without the foundation, there’s no challenge. Can I just move on?

JUDGE WOODCOCK: I think you move on.

JUDGE SCHEINDLIN: Good. OK. Made my day.

PROFESSOR CAPRA: We do rely on the adversary system to deal with this.

JUDGE SCHEINDLIN: And, in fact, we get very few challenges to photographs in real life. They just come right in.

PROFESSOR CAPRA: Let’s now go to Greg Joseph, for a proposal on detailed rules of authenticity for some kinds of electronic evidence.

---

MR. JOSEPH: So we have all this great stuff electronically. And a lot of stuff we want to get in. Judges, you know, are more or less familiar, depending on the judge, with how you get it in.

So Dan said, “Suppose we actually wanted to address the issue of authentication by drafting rules. And would you put something together?” So I said, “Of course.”

So here’s what I’ve got.36 We’re going to start with a rule which I call 901(b)(11),37 and it’s based on Rule 901(b)(6). Now, Rule 901(b)(6) is a completely unused rule these days. It’s about evidence of a telephone call that’s made to a person or to a business.38

So I thought emails would be a good analogy, and this one would be kind of the same notion for texts or online chats. Let’s just walk through. Evidence about an email communication as opposed to evidence about a telephone call.

So for an email communication, evidence that an email “bearing the customary format of an email,”39 because cases talk about it looking like an email. It’s got to look like an email to be an email.

“Including the email address of the sender and recipient.”40 So that by itself eliminates a lot of emails, right? We get all sorts of stuff, may go out—I send out little articles I write to about a thousand people. I don’t put everybody’s email address there. It’s just a blank. It just has the sender.

See app. II.

36. For Mr. Joseph’s PowerPoint presentation, see Appendix II.
37. Proposed Rule 901(b)(11) reads:
   (11) Evidence About an Email Communication. For an email communication, evidence that an email bearing the customary format of an email, including the email address of the sender and recipient:
   (A) was sent to the email address assigned at the time to a particular person, if circumstances, which may include some or all of the following, show that the person received the email: (i) A reply to the email was received from the email address assigned to the person; (ii) Subsequent communications with the person reflect the person’s knowledge of the contents of the email; (iii) Subsequent conduct of the person reflects the person’s knowledge of the contents of the email; or (iv) The person produced the email in the action.
   (B) was received from the email address assigned at the time to a particular person, if circumstances, which may include some or all of the following, show that the person sent the email: (i) The email contained the typewritten name or nickname of the recipient or the sender in the body of the email; (ii) The email contained the signature block or electronic signature of the person; (iii) The contents of the email would normally be known only to the person or to a discrete number or category of people including the person; (iv) Subsequent communications with the person reflect the person’s knowledge of the contents of the email; (v) Subsequent conduct of the person reflects the person’s knowledge of the contents of the email; or (vi) The person produced the email in the action.
See app. II.
38. Fed. R. Evid. 901(b)(6) (“For a telephone conversation, evidence that a call was made to the number assigned at the time to: (A) a particular person, if circumstances, including self-identification, show that the person answering was the one called; or (B) a particular business, if the call was made to a business and the call related to business reasonably transacted over the telephone.”).
39. Id.
40. Id.
So that’s excluded. But we’re talking about a very simple type. It’s bearing the customary format. It’s got a sender and a recipient.

There are two things I want to prove. One is if I say I sent it to Paul; and the other thing is, if I want to say Paul sent it to me, and I want to show he got it.

So the first part, (A), was the email “sent to the email address assigned at the time to a particular person?” That “assigned at the time” comes right out of Rule 901(b)(6). I used a particular person. This would work with a business, but I didn’t want to keep going forever on this.

“If circumstances, which may include some or all of the following, show that the person received the email.” And that follows the format of Rule 901(b)(6), but I didn’t try to—the language was slightly different, but it’s purely grammatical. So I want to show that I sent it and he received it. So what are the ways cases are looking at this, if we wanted to put it in rule format?

First, “A reply to the email was received from the email address assigned to the person.”

Now, “assigned to the person” is not actually an accidental kind of usage. That’s not talking about a Facebook page because that’s not necessarily assigned to the person. You could consider it that way.

You can also consider it to be something that a business, a public office, a regularly conducted activity, assigned to the person, which gives you some level of confidence, which you don’t have simply because somebody has a Facebook page, which we all know can be faked. And we have great examples that we use in our talks about that.

All right. So a reply is received from the email address assigned to the person. “Subsequent communications with the person reflect the person’s knowledge of the contents of the email.” You get a response. You get a phone call. You’ve communicated with the person that tells you that it was received.

“Subsequent conduct of the person reflects the person’s knowledge of the contents of the email.” And in the footnotes you’ll see examples: I said

41. See app. II.
42. Fed. R. Evid. 901(b)(6).
43. See app. II.
44. See app. II.
46. See app. II.
48. See app. II.
to Kevin, “Why don’t you meet me at the store at 9:30?” And Kevin shows up at 9:30. Right. He got the email. And if it was to rob the store, that would not be good.

“The person produced the email in the action,” which is a typical longstanding kind of way to show that there was an authentic document. It’s been produced by the other side.

All right. So now that’s to show that I sent it to Paul, and he received it.

Now, I got an email from Paul, and I want to show that he sent it. It came from his email address. So (B) says: “Was received from the email address,” again, “assigned at the time to a particular person, if circumstances, which may include some or all of the following, show that the person sent the email.”

So what do cases look at? First, “The email contained the typewritten name or nickname of the recipient or the sender in the body of the email.”

So in one of the cases that is in the footnotes there, Siddiqui, which was a 2000 Eleventh Circuit case, the sender always went by the name “Mo,” even though that wasn’t his name. And that was in the body of the email, and that was considered to be some evidence that Siddiqui had actually sent it.

49. See, e.g., Commonwealth v. Amaral, 941 N.E.2d 1143, 1147 (Mass. App. Ct. 2011) (“The actions of the defendant himself served to authenticate the e-mails. One e-mail indicated that Jeremy would be at a certain place at a certain time and the defendant appeared at that place and time. In other e-mails, Jeremy provided his telephone number and photograph. When the trooper called that number, the defendant immediately answered his telephone, and the photograph was a picture of the defendant. These actions served to confirm that the author of the e-mails and the defendant were one and the same.”) (citing MASS. G. EVID. § 901(b)(6)); see also State v. Glass, 190 P.3d 896, 901 (Idaho Ct. App. 2008) (same in the context of online chat).

50. See app. II.


52. See app. II.

53. See app. II.


55. Id. at 1321–23.

56. Id. at 1323; see also Donati v. State, 84 A.3d 156, 172 (Md. Ct. Spec. App. 2014) (“[A]n e-mail reference to the author with the defendant’s nickname, where the context of the e-mail revealed details that only the defendant would know, and where the defendant called soon after the receipt of the e-mail, making the same requests that were made in the e-mail.”); In re F.P., 878 A.2d 91, 95 (Pa. Super. Ct. 2005) (“He referred to himself by his first name.”); Commonwealth v. Capece, 17 Pa. D. & C. 5th 113, 119 (Ct. Com. Pl. 2010) (“The e-mails were often signed ‘Jerry,’ a name to which defendant answered.”); Shea v. State, 167 S.W.3d 98, 105 (Tex. Ct. App. 2005) (“Four of the e-mails were signed ‘Kev.’”).
All right. “The email contained the signature block or electronic signature of the person.”57 Again, any of this stuff can be easily faked, but we allow comparisons of handwriting. That can be easily faked. I’m sure somebody could forge my wife’s handwriting, which I’m intimately familiar with, and I would think it was hers. So “the email contained the signature block or electronic signature of the person.”58

“The contents of the email”—so now we’re looking at the contents—“would normally be known only to the person or to a discrete number or category of people including the person,”59 which is something that cases look at.60

Again, we’re talking about internal indicia of reliability. And one of those things is, well, he would know that or she would know that. Or only people that are in that particular function at that particular lab would know that.

“Subsequent communications with the person.”61 This is a complete parallel to what we had before. “Subsequent communications with the person reflect the person’s knowledge of the contents.”62

“Subsequent conduct of the person reflects the person’s knowledge of the contents,”63 or “the person produced the email in the action.”64

57. See app. II.

58. See app. II; see also Sea-Land Serv., Inc. v. Lozen Int’l, LLC, 285 F.3d 808, 821 (9th Cir. 2002) (holding that an email of one employee forwarded to party opponent by a fellow employee—containing the electronic signature of the latter—constitutes an admission of a party opponent); State v. Pullens, 800 N.W.2d 202, 229 (Neb. 2011) (“The signature or name of the sender or recipient in the body of the e-mail is also relevant to authentication.”).

59. See app. II.

60. See, e.g., Siddiqui, 235 F.3d at 1322 (“The context of the e-mail . . . shows the author of the e-mail to have been someone who would have known the very details of Siddiqui’s conduct . . . .”); Hardin v. Belmont Textile Mach. Co., No. 3:05-CV-492-M, 2010 U.S. Dist. LEXIS 61121, at *16 (W.D.N.C. June 7, 2010) (“The e-mails also discuss ‘various identifiable matters’ related to [plaintiff’s] employment . . . which sufficiently authenticate the e-mails as being ‘what its proponent claims.’” (quoting United States v. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006)); Safavian, 435 F. Supp. 2d at 40 (“The contents of the e-mails also authenticate them as being from the purported sender and to the purported recipient, containing . . . discussions of . . . Mr. Safavian’s work at the General Services Administration (‘GSA’), Mr. Abramoff’s work as a lobbyist, Mr. Abramoff’s restaurant, Signatures, and various other personal and professional matters.”); Pullens, 800 N.W.2d at 229 (noting inclusion of sender’s social security and telephone numbers); State v. Taylor, 632 S.E.2d 218, 231 (N.C. Ct. App. 2006); Shea, 167 S.W.3d at 105 (describing several connections between emails and complainant’s interactions with defendant); Massimo v. State, 144 S.W.3d 210, 216 (Tex. Ct. App. 2004) (“[T]he author of the e-mails knew the subject of the investigation, harassing e-mails, before Sparby revealed that to her.”).

61. See app. II.

62. See app. II; see also Dominion Nutrition, Inc. v. Cesca, No. 04 C 4902, 2006 U.S. Dist. LEXIS 15515, at *16 (N.D. Ill. Mar. 2, 2006) (“E-mail communications may be authenticated as being from the purported author based on . . . other communications from the purported author acknowledging the e-mail communication that is being authenticated.”) (citing Fenje v. Feld, 301 F. Supp. 2d 781, 809 (N.D. Ill. 2003)); Shea, 167 S.W.3d at 105; Bloom v. Commonwealth, 542 S.E.2d 18, 20–21 (Va. Ct. App. 2001).

63. See app. II; see also Commonwealth v. Amaral, 941 N.E.2d 1143, 1147 (Mass. App. Ct. 2011) (“The actions of the defendant himself served to authenticate the e-mails. One e-mail indicated that Jeremy would be at a certain place at a certain time, and the defendant appeared at that place and time. In other e-mails, Jeremy provided his telephone number and
Now, that kind of approach, which I’m sure the committee could do much more thoroughly and much better and could identify other characteristics as well, could be used also for texts. It could be used for online chats because the kinds of criteria that I’m drawing from in these cases and other cases are applied to those. There just happened to be more cases that deal with emails, although there are a lot of cases about online chats, as well.65

So that was email, texts, and potentially chats.

Now websites. Let’s talk about website contents because you want to get the website into evidence. We’re obviously not talking about a government website because that’s self-authenticating under Rule 902(5).66

So first of all, I’m limiting this to a business, a public office, or other organization. I’m intentionally eliminating Facebook, MySpace, Twitter, all of these things where I can go online and say, “I’m George Paul” and just say whatever I want and send emails from that. Although, the email rule would—I’ve tried to address those kinds of emails.

So, evidence about website contents. “For a webpage from the website of a business, public office or other organization,”67 however you describe a regularly conducted activity, “a printout or other output readable by
That language is, of course, stolen from Rule 1001(d) because we know that a printout or other output readable by sight is an original.69

“A printout or other output readable by sight bearing the internet address and the date and time the webpage was accessed and the contents of the exhibit downloaded.”70

That’s something that a lot of cases look at. There are a couple of cases in Oregon, most recently in January this year finding an insufficient showing of authenticity.71 And one of the things that the judge looked at was, it doesn’t state on the exhibit the website address and the date and time that it was downloaded.72 It just doesn’t show that.

So that’s something that courts look at. It also gives the court, as we’ll see later on, an opportunity to actually verify if it’s still up, but that will be one of the factors we’ll look at.

So it has those characteristics. It’s from a regularly conducted activity. It’s a printout. It bears the internet address, the date and time.

And then we have the following three provisos with subdivisions. The first is: “A witness testifies or certifies.”73 This is going to be the prima facie foundation. And this is language, of course, stolen from Rules 902(11) and (12):

A witness testifies or certifies in compliance with a federal statute or rule prescribed by the Supreme Court that: (i) The witness typed in the Internet address reflected on the exhibit on the date and at the time stated; (ii) The witness logged onto the website and reviewed its contents; and (iii) The exhibit fairly and accurately reflects what the witness perceived . . . .74

And that’s what all the cases say, that’s prima facie.75 You have to have that or I’m not even going to look at this thing. So that’s the first thing. You’ve got that certification or testimony.

---

68. See app. II.
69. Fed. R. Evid. 1001(d) (“An ‘original’ of a writing or recording means the writing or recording itself or any counterpart intended to have the same effect by the person who executed or issued it. For electronically stored information, ‘original’ means any printout—or other output readable by sight—if it accurately reflects the information. An ‘original’ of a photograph includes the negative or a print from it.”).
70. See app. II.
71. See Estate of Konell v. Allied Prop. & Cas. Ins. Co., No. 3:10-cv-955-ST, 2014 U.S. Dist. LEXIS 10183, at *3 (D. Or. Jan. 28, 2014) (“To authenticate a printout of a web page, the proponent must offer evidence that: (1) the printout accurately reflects the computer image of the web page as of a specified date; (2) the website where the posting appears is owned or controlled by a particular person or entity; and (3) the authorship of the web posting is reasonably attributable to that person or entity.”).
72. Id. at *4.
73. See app. II.
74. See app. II.
The second thing, the exhibit bears internal indicia of reliability. “Indicia of reliability, which may include,”76 and I’ve just picked a number of them that I’ve seen in cases.

First, “Distinctive web site design, logos, photos or other images associated with the website or its owner.”77

If you go to Chevrolet.com, you’re going to expect to see a Chevy symbol on that website. Right.

Number (ii), “The contents of the webpage are of a type ordinarily posted on that website or websites of similar entities.”78 So if I go to Chevy.com, and I’m assuming there is such a place. I haven’t gone looking at it. I’m expecting to see cars. And I would expect if I went to Ford.com, a similar entity or similar website, I’d see that. So it’s got the logo. It’s the sort of thing I would expect to see on that website.

“(iii) That the contents of the webpage remain on the website for the court to verify.”79 That actually has two aspects to it. First, the court can actually see that it’s there. But second, it really reduces any possibility that it was hacked, because why would it still be there? You know, that should have been removed if there’s any claim by the owner of that website that it’s not something that he or she or it is responsible for.

“(iv) That the owner of the website has elsewhere published the same contents, in whole or in part.”80

“(v) That the contents of the webpage have been republished elsewhere and attributed to the website.”81 That would, of course, raise the authenticity of the republication, but that’s just another exercise going through the same thing.

“(vi) The length of time the contents were posted on the website.”82 Again, that’s another indication; if it was up there for a year and a half, that’s not hacker material. There has to be some good explanation why it was allowed to stay there if the owner or proprietor is disclaiming responsibility for it.

And then (C), you have to give notice to the other side. That just picks up just as (A) started with the 902(11), (C) concludes with the 902(11), that you give advance notice so the other side can contest because there always can be phony material that’s put on a website.83

Now, I also did a couple things because I was doing Rule 901, why not do Rule 902. So email. I see cases that do not tell me how, but tell me that an email is self-authenticating.

And they’re not talking about it. They’re not saying there are distinctive characteristics. They’re not saying it’s got the “@” symbol, right, which

76. See app. II.
77. See app. II.
78. See app. II.
79. See app. II.
80. See app. II.
81. See app. II.
82. See app. II.
83. See app. II.
tells me that it’s a trade inscription or mark. The cases just say they’re self-authenticating.84

So what I’m suggesting here, it’s really just the first sentence. The second sentence is just Rule 902(11). “The email bears the customary format of an email and purports to issue from the email system of a business, public office or other organization . . . and not from a public email system.”85 Not from Gmail, not from Yahoo!, not from someplace any of us could go and use anybody else’s name.

I suggest to you that if I get an email in the ordinary course of business from another law firm, and it says it’s from another law firm, that’s 99 times out of 100 going to be from another law firm.

You know, what are the odds that somebody’s going to take Davis Polk’s website and come up with a phony email from that? That doesn’t tell me that the person was actually at his or her desk and actually typed the email. It doesn’t tell me a whole lot of things, but that I actually got an email. Do we have to actually go further than that on a simple email?

And for a text, do you really have to go further than say it looks like a text, it comes from this phone number? Now, I don’t know, maybe my wife didn’t have her phone that day, but it comes from that phone number. Is that not enough at a very beginning level to self-authenticate and let the opponent come in and say, “I wasn’t there at the time. I didn’t have access to my phone.” Whatever.

So a few ideas for the committee to think about.

PROFESSOR CAPRA: Thank you, Greg. I have a question about the website rule. You have the witness testifying or certifying, and you also require indicia of authenticity such as distinctive characteristics.

MR. JOSEPH: All these are “ands.” There’s an “and” for each one.

PROFESSOR CAPRA: I’m just thinking out loud as to why (A) wouldn’t be enough or (B) wouldn’t be enough. In other words, maybe an “or” should be, what do you think about an “or”? Would that be inconsistent with the case law?

---


85. Proposed Rule 902(13)–(14) reads:

The following items of evidence are self-authenticating; they require no extrinsic evidence of authenticity in order to be admitted:

(13) Email. The email bears the customary format of an email and purports to issue from the email system of a business, public office or other organization (regularly conducted activity) and not from a public email system. Before the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the email so that the party has a fair opportunity to challenge it.

(14) Text Message. The text message bears the customary format of a text message and purports to emanate from a number or other unique source designation assigned at the time to a particular device. Before the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the text message so that the party has a fair opportunity to challenge it.

See app. II.
MR. JOSEPH: That’s a fair point. You probably could do (A) or (B), thinking about that.

PROFESSOR CAPRA: It seems to me otherwise you’re requiring a stronger showing than actually required under the low standards of authenticity.

MR. JOSEPH: I think that’s a fair point.

PROFESSOR CAPRA: Well, this is really helpful. I think this is a great starting point for the Advisory Committee. I’m going to mark this up for the Committee’s next meeting.

MR. VORDER BRÜEGGE: One point on having the witness testify that they logged into the site.

MR. JOSEPH: Is that bad locution?

MR. VORDER BRÜEGGE: Well, there’s certainly—I mean, I just wonder about the issue of bots that go out and pull down websites automatically for later analysis.

MR. JOSEPH: You know, you’re talking about like Archive.org.

MR. VORDER BRÜEGGE: Archive.org or Wayback Machine.

PROFESSOR CAPRA: Wayback Machine.

MR. JOSEPH: That is Archive.org. That’s the same thing. This doesn’t address that because that would be a scientific process. I think that would just be a Rule 901(b)(9) kind of a process.

PROFESSOR CAPRA: That’s right.

MR. JOSEPH: And, in fact, at least two courts have taken judicial notice of the Wayback Machine lately.

PROFESSOR CAPRA: Including somebody here; right? Was that you, Judge Scheindlin?

JUDGE SCHEINDLIN: Yes.

PROFESSOR CAPRA: You don’t need a new rule for that, essentially.

MR. JOSEPH: Right. I think that’s covered. I mean, the real question is: Do you want to be helpful without being ridiculous about it because you’re writing a rule of evidence, not a treatise?

PROFESSOR CAPRA: Right. It’s a theoretical question because you could get all this from the case law if you took about 100 years to do it; right?

MR. JOSEPH: I would hope not quite 100. Sixty-three so far.

---

86. “The Internet Archive is a 501(c)(3) non-profit that was founded to build an Internet library. Its purposes include offering permanent access for researchers, historians, scholars, people with disabilities, and the general public to historical collections that exist in digital format.” About the Internet Archive, INTERNET ARCHIVE, https://archive.org/about/ (last visited Nov. 26, 2014).


PROFESSOR CAPRA: I guess the question then is as Judge Sutton was saying, by the time you codify, now you have new things to do and you end up with having to constantly amend by adding new factors to the list that the rule sets forth.

MR. JOSEPH: All fair points. That’s why I left it with the ones that have been ubiquitous for a good while and seemed to be likely to be ubiquitous.

You might want to have a definition in Rule 101 that applies these principles to new forms of communication as they develop.

JUDGE DIAMOND\textsuperscript{89}: When you’re talking about putting these in rules, and as Judge Sutton pointed out, taking five years for these rules to become rules, isn’t there a real danger when you’re this specific that the rule is going to be obsolete just with its use of language by the time it’s adopted? For example, referring to typing in a URL, by the time the rule gets adopted, people may be dictating everything.

MR. JOSEPH: I agree with that 100 percent.

JUDGE DIAMOND: Logged onto is another example.

MR. JOSEPH: You’re absolutely right. And I did not try to—in the cover note, the disclaimer that was written, I said I’m not trying to draft with the kind of precision you would have to draft with. I’m trying to put out concepts here. But I think that’s a critical point.

What you really want to say is that the witness “accessed,” or you even want to put it in the passive: “The internet address was accessed.” I agree with you on the drafting point.

PROFESSOR CAPRA: It’s like you need an IT person to help you draft the rule.

MR. JOSEPH: Clearly.

PROFESSOR BROUN\textsuperscript{90}: Just a real quick question. Are there outlier cases that go other directions in this, in your sixty-three years of looking at this?

MR. JOSEPH: Listen, you’ve got that case by the judge who has been impeached down in Texas saying that there’s nothing of any value on the internet, and I’m never going to rely on it for anything because anybody can put anything on the internet.\textsuperscript{91}

But there are—so the answer is, of course, there are. But I’ve tried to be fair on what most cases are saying, but there’s no question. And it’s like we

\textsuperscript{89.} Judge Paul Diamond is a member of the Civil Rules Committee and serves as that committee’s liaison to the Evidence Rules Committee.

\textsuperscript{90.} Professor Ken Broun is a consultant to the Evidence Rules Committee.

\textsuperscript{91.} See St. Clair v. Johnny’s Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 775 (S.D. Tex. 1999) (“ Anyone can put anything on the Internet. No web-site is monitored for accuracy and nothing contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on any web-site from any location at any time. For these reasons, any evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of the hearsay exception rules . . . .”).
say in New York where we have four million cases filed every year, “You can find a case that says anything.”

MR. MURRAY: We’re struggling with this in Maine, of course. You’re trying to identify various kinds of facts and circumstances that relate to each one of these technologies that might be helpful in determining whether or not it was authentic.

And I join those who question whether or not we should make this so technologically kind of linked and rather merely say, “It is authentic if a review of the facts and circumstances associated with that technology gives reason to believe—”

MR. JOSEPH: Peter, I think we have that already. So I would agree. If that’s the conclusion that the Committee comes to, then whether it’s Maine or the committee that is assembled here, then you don’t do anything.

PROFESSOR CAPRA: I was just thinking as you were—as you made your presentation, Greg, it might be a good idea to think about amending the telephone rule to just add these other forms of communication.

MR. JOSEPH: Putting them all together, yeah. Right. I agree. Then just make it for communication.

PROFESSOR CAPRA: Yeah. Right.

JUDGE SUTTON: I’m just curious. I love what you’re doing. This is so helpful. But what is your advice on this question? Do we just look at (a) and say, “Listen, (a) has a standard. It’s not a rule.” Which would you prefer?

MR. JOSEPH: I would draft it up and look at it and see if it really is beneficial at the end of the day. I will tell you, I think that there is benefit if you can do it right because I think it would be helpful to judges and to lawyers.

And I think that the current level of generality isn’t that helpful. I mean, it’s critical so that you have the right—when you’re actually in a case, to make your arguments, and you’re not going to ever take away Rule 901(a), or you’re not going to take away Rule 901(b)(4). You’re going to have the general.

But I would give it a shot, taking into account what Judge Diamond said, and you know, all the points that people are making. Maybe you don’t want to talk about an email communication. Maybe you want to talk about a transmitted communication the way Dan is talking about.

JUDGE SUTTON: We went through the whole rule and tried to use the verb “transmit” to account for electronic communication. We couldn’t settle on it. We could not figure out how to do this. And that was with the technology we understood today. That was without even trying to anticipate future developments. We just said we can’t do this.

MR. JOSEPH: Then make it electronic and then define electronic to mean everything.

92. Professor Peter Murray, of the University of Maine, was a member of the audience.
JUDGE WESLEY: Wouldn’t you want to have the rule have an additional provision that says any other factor that relates to the authenticity? Because human experience has this wonderful way of lining up the tumblers differently. As soon as you announce a rule, the deviations from it or the exceptions from it begin to develop.

MR. JOSEPH: I agree with that. I did add the phrase “which may include.” But I think being even express about it is really important. Because you’re right, once it’s written down, then people will be looking at that.

PROFESSOR CAPRA: Judge Woodcock.

JUDGE WOODCOCK: I think this may be a wonderful permanent solution to a temporary problem. And what I’m going to do, you know, as a trial judge, you get an objection to something like an email or a website, and you walk over to the side. And you’ve got the jury sitting here, and you’re whispering down. You’re trying to figure out people using language you don’t understand.

And I’m going to copy this, and I’m going to have it as a list to go through. But I’m not sure that over the course of the next few years it doesn’t, one, become obsolete. That it may be too specific. And one of the geniuses of the Federal Rules is that they’re so general that they can be applied to different things.

So I think it takes the ball down the road, down the field a little bit, and it’s helpful. But I think basically what you’ve done is compiled case law that will catch up to Rule 901(a) in the long run.

MR. JOSEPH: That’s the issue.

PROFESSOR CAPRA: That’s the issue. If nothing else, it’s really great to have brought up all that case law and put it into rule format. I thought it was a fascinating piece of work seeing all those cases essentially codified.

MR. JOSEPH: You have to say that. You made me do it.

PROFESSOR CAPRA: I know. Thought I’d just help you there. Thank you so much, Greg. We’ll move to John Haried for a suggestion with respect to an authenticity issue that he’s going to discuss.

MR. HARIED: I think we’re going to see a lot of similarities between what Greg just did and what I’m proposing. I’m going to make two proposals. And they’re based upon three facts that I think are true. And I think all of us have the same experience.

The first is that in this new electronic world, machines are generating information more than people. That’s going to be important evidence in our cases.

Second, that in an electronic world, the custodians of those records are disbursed across the country and indeed, across the world. So it creates all

---

93. Judge Richard Wesley is a member of the Committee on Rules of Practice and Procedure (the Standing Committee) and is that committee’s liaison to the Evidence Rules Committee.

94. For Mr. Haried’s PowerPoint presentation, see Appendix III.
kinds of logistical and expense issues for authenticating electronic information in litigation.

The third is that in many instances, there is no genuine dispute about the authenticity of electronic information. And for that reason, anything that helps lawyers get to the conclusion or get to the decision whether an exhibit is going to be challenged for authenticity before trial is a good thing.

So just to start out, I want to make sure that you all understand. This is Haried’s thinking. This is not the Department of Justice’s proposal. And there shouldn’t be any confusion about that.

So my first proposal is that—and this came up just a moment ago, with respect to a process or system that produces a reliable result. With regard to machine-generated information, that’s a perfect opportunity to have an out-of-court certification process that helps the parties identify early whether there’s going to be a real dispute about the authenticity of this evidence or not.

What’s the hole that I’m trying to fill here? Well, we have out-of-court certifications under Rule 902(11) for certified domestic records, under Rule 902(12) for certified foreign records.

And I’m suggesting there’s a hole here that could be filled and would help lawyers and the court grapple with the authenticity issues earlier than trial and address them.

So I’m going to use for an example a recent prosecution, the Bradley Manning case. Mr. Manning was an employee of the U.S. Army and was accused of leaking classified information to WikiLeaks. And this involves the Wayback Machine which we just were talking about a few moments ago. This was litigated last year.

And here is a screenshot of the Wayback Machine. It’s on an internet site called Archive.org. The Internet Archive’s automated machinery goes across the web and captures webpage images all the time. They’re up to 402 billion images.

All you have to do is go into the search box and type in information, and it will lead you on a series of steps to find historical webpages.

---

95. Fed. R. Evid. 902(11) (“The original or a copy of a domestic record that meets the requirements of Rule 803(6)(A)–(C), as shown by a certification of the custodian or another qualified person that complies with a federal statute or a rule prescribed by the Supreme Court. Before the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the record—and must make the record and certification available for inspection—so that the party has a fair opportunity to challenge them.”).

96. Id. 902(12) (“In a civil case, the original or a copy of a foreign record that meets the requirements of Rule 902(11), modified as follows: the certification, rather than complying with a federal statute or Supreme Court rule, must be signed in a manner that, if falsely made, would subject the maker to a criminal penalty in the country where the certification is signed. The proponent must also meet the notice requirements of Rule 902(11).”).

97. Editor’s note: the judicial decision was not available before this issue went to print.

98. See app. III.
And in the Bradley Manning prosecution, the government did that. They went to the Wayback Machine. They were looking for anything that would connect Bradley Manning to WikiLeaks.

And they found this page. This is Exhibit 109. You can see it’s got a stamp over there. And it is a screenshot of a WikiLeaks’s webpage from November 5, 2009.

And it’s laid out by country. There’s a whole list of some thirty-three different countries and international organizations that, according to this image, WikiLeaks was trolling for sensitive, confidential, or classified information.

And this is just the header from the top of this exhibit just so you could read it. It appears to be a solicitation.

So the question was in this case, was this Exhibit 109 an authentic record? The government wanted it because under the heading “United States” and that list of thirty-three countries and organizations, these are the things that this image said WikiLeaks was looking for, some of which is classified information, and some of which was actually the same types of information that Bradley Manning was accused of downloading and passing on to WikiLeaks.

In the judge’s opinion in this case, she cited these seven cases. I think there are others out there. There are new ones since this came out. I put this up here for a couple reasons, but principally to show that the whole issue of authenticating webpages and particularly this webpage, the Wayback Machine webpage for historical webpages, is something that’s coming up frequently in litigation.

MR. JOSEPH: John, just on that, most of those would have somebody from Archive.com or Archive.org testifying, right?

MR. HARIED: That is correct. In fact, in most of those cases, they said authentication should be by a witness with knowledge.

And, in fact, in her opinion, the judge in the Manning case reached that conclusion and said the way to authenticate this exhibit is to bring an Archive.org knowledgeable custodian, have the person come into court and testify.

The Manning trial was occurring in, I think, Baltimore or somewhere in Maryland, one of the military bases. And Archive.org is in San Francisco.

99. See app. III.


101. See cases cited supra note 100.
So the witness would have had to come all the way across the country, just to authenticate an apparently authentic webpage.

The other paragraph I put up here was just part of her opinion in which she said, “You’re going to have to call a live witness. But if you do, I believe that this exhibit would be relevant because the government has put on other evidence demonstrating that Bradley Manning searched for on his computer information about WikiLeaks and had contact with WikiLeaks personnel.”

So the story in this case was the government subpoenaed the Archive.org custodian of records, was all set to bring that person from San Francisco to Baltimore to testify. Did that on a Friday.

On Monday, the defense attorneys walked into court and stipulated to the authenticity of that webpage. For whatever reasons, I’m sure there’s a whole back story, but that—I think that’s significant because that’s sort of a common experience. When push comes to shove, the lawyers figure out whether they have a real dispute or not.

And that’s one of the—of course, one of the advantages of the courtroom, but I think it’s also one of the advantages of an out-of-court certification process because it forces, of course, the proponent and the opposing party to come to grips with, “Am I really going to fight about this exhibit, and do I have my ducks lined up?”

So my suggestion is, and much like Greg’s, this is very preliminary, very rough drafting, not drafted to the standards of this committee, but just to set out some ideas about how a rule might be constructed.

And basically, what I’ve done is kept the general framework of the business records exception in Rule 803(6) and the rules for self-authentication of business records in Rules 902(11) and (12), and applied it to machine-generated information.

So the first would simply be that “the record was generated at or near the time by a machine utilizing a process or system that produces an accurate result.” That’s the Rule 901(b)(9) standard.

And that it generally looks like a business record because it’s part of a regular activity and was part of the duties of the organization to gather this type of information.

The proposal provides for a certification out of court and compliance with the notice requirements of 902(11). So it builds in many of the

---

102. Proposed Rule 902(13) reads:
Certified Records of Regularly Conducted Activities Generated by a Machine.
The original or a copy of a record if:
(A) the record was generated at or near the time by a machine utilizing a process or system that produces an accurate result;
(B) the record meets the requirements of Rule 803(6)(B), (C), and (E);
(C) as shown by a certification that meets the certification requirements of Rule 902(11) for domestic records or Rule 902(12) for foreign records.
The proponent must also meet the notice requirements of Rule 902(11).
See app. III.
103. “Before the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the record—and must make the record and certification
same procedural steps and qualifications to mimic Rules 803(6) and 902(11), but changes it to just information generated by a machine.

And then I put together a second proposal about an out-of-court certification. And that allows a proponent to authenticate a copy of an electronic record via an out-of-court certification.

And this is done all the time in the electronic world. And the principal way of certifying a copy is to use what’s called a hash function.

And again, what’s the hole? The same idea that there could be an out-of-court certification that would address copies of electronic devices, storage media, and files.

So the hash function. It’s basically a mathematical algorithm that’s contained in software. The software examines every detail, every zero and every one of an electronic device, whether it’s a memory on a cell phone, hard drive on a computer, or a picture, child pornography picture or any other kind of electronic file, and assigns a unique value to that item. So the question is: How unique is that?

Let me tell you how hash value is used typically in the electronic—particularly the e-discovery world. It’s one way of removing duplicate emails from a whole collection of emails. If you have 100,000 emails, many of which were sent to the same recipients who produced it, you can use a hash function to eliminate duplicates or to verify the integrity of a file that’s been transmitted electronically. You can determine that what the sender sent was exactly what the receiver received.

It comes up in litigation in different ways. But one principal way is, if a storage media like a hard drive or a cell phone is seized as evidence, or is evidence in a case and then copied for analysis to be presented in court, that copy can be verified using the hash function.

That’s important because forensic examiners typically don’t want to work with the original for fear of altering it in some way and spoliating it.

So just to demonstrate the value of hash function, I’ve taken the Preamble to the U.S. Constitution in its original form and created two altered documents—using two different software programs for hashing, what the hash value is.104

These are substantially the same type of software that’s commonly used in the industry to set a hash value. You can see it, a long string of letters and numbers.

Now, if we take that same Preamble and we remove the period at the end and then run the software again, so we get a different set of hash functions. And if we leave a space, but remove the period, a second alteration of the original, you get yet a third unique value under either of these two prevalent softwares.

available for inspection—so that the party has a fair opportunity to challenge them.” FED. R. EVID. 902(11).

104. For this discussion, please refer to Appendix II.
So there’s the comparison. You can see how just that minor change made in these hash values can become unique identifiers for an electronic file.

So the rule that I suggest to help in this area allows for a qualified person to authenticate by way of certificate. And the reason it is important is because oftentimes, the person making the copy is not the analyst. So it would save bringing two people to court to authenticate and testify about an exhibit if the out-of-court certification process was available.

PROFESSOR CAPRA: You mean you’d call the analyst and not—

MR. HARIED: You could just call the analyst and not call the technician that copied the file. Right.

So simply, again, using many of the same standards from Rules 803(6) and 902(11) and (12), but saying if you can demonstrate by a certificate that the copy is true and accurate by a reasonable means, and that could be a hash function or some other methodology, and there’s no reason to suspect that the information is untrustworthy, you’re doing a certification, and provide for a notice requirement, you could eliminate what are really unnecessary witnesses, assuming there’s not a genuine dispute.105

PROFESSOR CAPRA: Thank you, John. That’s great. We have comments or questions. Paul Shechtman first, then Judge Grimm.

MR. SHECHTMAN: My first one is this, and my last one. I should know the answer to it, but as to the existing certifications, like Rule 902(11), what about Crawford objections?

JUDGE GRIMM: That’s the problem.

MR. SHECHTMAN: And before we’re adding new ones, I mean, it’s fine in civil cases, but I take it really we’re not going to help you very much if these are all inadmissible under Crawford.


JUDGE GRIMM: You first. You’re the professor.

PROFESSOR CAPRA: So Yeley-Davis107 is a leading case in the Tenth Circuit that says that these certificates of authenticity are not testimonial under Crawford because even though they are prepared for trial they do nothing more than authenticate another document.

And the Court in Melendez-Diaz v. Massachusetts108 recognized an exception to the Confrontation Clause when a certificate does no more than

105. Proposed Rule 902(14) reads:
Certified Copy of Electronic Device, Storage Media or File. A true and accurate copy of an electronic device, storage media or file if:
(A) the copy is true and accurate as shown by a reasonable means; and
(B) the record meets the requirements of Rule 803(6)(E);
(C) as shown by a certification that meets the certification requirements of Rule 902(11) for domestic records or Rule 902(12) for foreign records.
The proponent must also meet the notice requirements of Rule 902(11).

See app. III.

107. United States v. Yeley-Davis, 632 F.3d 673 (10th Cir. 2011).
authenticate another document—as opposed to the certificates in *Melendez-Diaz*, which certified the results of a forensic test.

And every case that I’ve seen says that this certification process does not violate the Confrontation Clause. That’s not to say there wouldn’t be a case later on that doesn’t present the issue.

JUDGE GRIMM: *Melendez-Diaz* did say that—there was a discussion about all of the—it was done in the chain of custody concept.\(^{109}\) You don’t need to have every single thing necessary to authenticate.

But where it’s interesting is at some point that we have the explanation as to how the hash value was applied. Is that more than authenticating the document? That issue may come up until it’s been resolved, not as dicta in a decision where it was the end report, which was *Melendez-Diaz*, but on the question of authenticity.

Civil cases are a different story. Under Rule 103, the court can make a pretrial definitive ruling on the record. So you can do all of this in a civil case and have affidavits from the people who did it, not have to bring them in.

Because again, under Rule 1101(d)(1), and also under Rule 104(a), the Rules of Evidence, except for privilege, don’t apply to the court to make a determination. Where it gets a little bit different is when you have a situation where it’s a criminal case, and you have Confrontation Clause issues.

And I’m not so sure that after *Williams*\(^{110}\) that the comment in *Melendez-Diaz* is as clear as it was when *Melendez-Diaz* was written. That’s my concern.

PROFESSOR CAPRA: Well, you know, the other thing is, this actually might be one of the places where rulemaking—the length of rulemaking is useful because you can wait and see what the case law is doing.

But does anybody have any other questions or comments? Rick Marcus.

PROFESSOR MARCUS\(^{111}\): There’s a doctor who is stating at e-discovery events that software used to make medical records automatically says a lot of things happen that didn’t happen.

How would you deal with that? Maybe machines don’t always produce reliable things. Maybe they produce things that are really unreliable.

MR. VORDER BRUEGGE: I have a perfect example of that that goes back to this photographic issue. Hewlett-Packard produced a digital camera several years ago that would allow you to take a photograph of a person and then make them thinner on the record and then save the image file.

You can see why there would be a market for it. But when that digital file was written to that camera’s memory, the original image was the altered image because one had acted on it within that camera.

\(^{109}\) Id. at 335–36.


\(^{111}\) Professor Richard Marcus is a Reporter to the Civil Rules Committee and was in the audience at the symposium.
PROFESSOR CAPRA: How does that work for hash marks and the like?

MR. VORDER BRUEGGE: The hash is only going to be applied to that altered image.

PROFESSOR CAPRA: But what can a witness do about that? In other words, what kind of a benefit would a witness be to deal with that particular issue? Is somebody going to ask him about the altered image? Would they know?

MR. HARIED: I think it’s the same answer as before. There can always be the one off, but for the 98 percent or 99.9 percent, this could work well.

How you deal with those questions of alteration, that would require very knowledgeable counsel to know which questions to ask and not to agree to a certification and say, I want to challenge this. And that would be appropriate. I think the advantage of the certification process is, it raises those issues and puts people on notice and gets the issues addressed before the trial starts.

PROFESSOR BROUN: This would simplify things a good deal. I still see Daubert issues with regard to reliability of this process.

MR. HARIED: I think that’s absolutely right. And I think it’s up to the lawyers to raise those issues.

MR. JOSEPH: Not necessarily. There are two ways of looking at—particularly, digital alteration or digital enhancement cases would say—there are two lines of cases. One would say first, you have to deal with Daubert. 113

Another would say, you can go right to the second step; and that is, you can go right to reliability. Is that used by, say, the business community in the ordinary course of business? Is it relied upon so frequently that you can assume reliability?

So you might be able to avoid Daubert. It’s a function of approach. You definitely have to make sure that the underlying software is authentic.

PROFESSOR CAPRA: In terms of schedule, we’re going to finish authenticity, and then we’ll take a break. So Richard, you’re next.

Thanks very much, John, that was great.

MR. VORDER BRUEGGE: This is a fascinating topic and one that I find to be of great importance in what we do in the criminal justice system as well as in the civil system. I don’t spend much time working on civil cases. I don’t know that I’ve ever worked on a civil case. But I was invited here today to talk about biometrics playing into authenticity.


113. See, e.g., United States v. Christie, No. 07-332 (HAA), 2009 WL 742722, at *1–6 (D.N.J. Mar. 18, 2009) (applying Daubert and admitting expert testimony to distinguish “virtual child pornography” from the real thing); United States v. Frabizio, 445 F. Supp. 2d 152, 154–60 (D. Mass. 2006) (applying Daubert and finding that “[i]f photographic experts as a general matter are inadequate to the task of identifying computer-generated images, then no level of experience in that field will suffice to qualify one as an expert”).
Before I begin, I want to make it absolutely crystal clear that I am not speaking on behalf of the Federal Bureau of Investigation or the Department of Justice or any part of the U.S. government.

These are purely my thoughts and ideas. I did run these slides by Office of the General Counsel attorneys at the FBI, however, for fact clarification and to make sure that I wasn’t going to trip over myself for that.

So not being sure of what my colleagues were going to speak about earlier today, I thought I would make this point of differentiating integrity from authenticity.

I frequently lecture on image and video manipulation and probably testified about anywhere from ten to twenty times in child pornography cases regarding the authenticity of images and videos. And so explaining this is something that’s important to me.

Also, many people in law enforcement get tripped up by the issue of integrity versus authenticity. And there are a lot of vendors out there who would like to sell products that they pitch as authenticating evidence when, in fact, it merely demonstrates the integrity of the evidence.

And the analogy came from colleagues in Germany, actually, the Bundeskriminalamt, the FBI equivalent in Germany, talk about the king’s scroll example.

So back in the Middle Ages, you would have the king, who would write a document up and sign it and then roll up the scroll and seal it with wax and imprint it with his signet ring or whatever.

The seal is what verifies the integrity of that document. When that seal is in place, that means that document has not been unrolled and altered in any way. The integrity is there.

Authenticity has to do with the king’s signature on the bottom saying, “This is what I said, true and accurate depiction.”

So integrity can always be a component of authenticity. But you see I have the caveat in here, it’s not necessarily always going to be a component.

Because I work with a lot of video and closed-circuit television systems, and many of you who work with computer forensic experts know, and John went through it wonderfully, the hashing is critical.

The first thing you do is you preserve that evidence. You protect it. But in the case of closed-circuit television evidence, you cannot necessarily always recover the highest quality video from a hashed copy of that hard drive. You have to actually engage with the system to extract the video evidence because there are players issues, there are codec issues.

And so best practice for the forensic examiner withdrawing video is to actually alter that evidence in a way when recovering it. Once that is then recovered, it can be hashed and verified, but there are processes in place.

114. For Mr. Vorder Bruegge’s PowerPoint presentation, see Appendix IV.
So the integrity, this hashing function that John so brilliantly explained earlier, is the gold standard. And I use that term quite intentionally, gold standard, because most commonly in forensics, we hear about DNA being the gold standard. I would put to you that hashing exceeds DNA in terms of being a gold standard for integrity verification.

So why am I here today? It actually has to do with biometrics. And the federal government has been looking at biometrics quite extensively over the last twenty years or more.

The definition you can see here comes from the biometrics.gov website\textsuperscript{115} that was put together by the National Science and Technology Committee’s Subcommittee on Biometrics and Identity Management, measurable biological, meaning anatomical and physiological or behavioral characteristics used for identification of an individual.

And I’ve separated these two into anatomical only versus behavioral and anatomical specifically because the question of handwriting came up in bringing me here.

We’re all familiar with DNA, fingerprints, face recognition, iris recognition. Vascular patterns I add simply because in the Far East, the use of vein patterns on the back of the hand is a pretty widely accepted biometric. It’s also used somewhat in this country, casino settings, various security access applications.

Behavioral. Voice and speaker is one that goes—is quite frequently of interest. Gait, how a person walks is frequently referred to as a biometric that may be of use.

And finally, we get to handwriting and signature, both the dynamic aspect of it as well as just if you were to compare your signature today, how would it look compared to a signature you had thirty years ago.

Not an exhaustive list. Let’s talk about some of the ideal characteristics of biometric signatures. You would very much like them to be persistent over a lifetime, OK, from infancy to senescence.

You would really like it to have a high ability to individualize. There are more than seven billion people on this planet. From the standpoint of implementing a system that is going to be used, either in a court setting or other setting, you want it to be easy. You don’t want it to cost a lot. You want to be sure that people are going to be willing to use it.

Finally, you also have to be concerned about how easy it is to fool the system and whether the biometric that you are going to use can be kept private; because if you can’t keep your biometric private, it’s going to make it a lot easier to spoof the system unless things are built into the system to prevent that.

\textsuperscript{115} “As a general term used alternatively to describe a characteristic or a process. As a characteristic: A measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition. As a process: Automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.” Nat’l Sci. & Tech. Council, Comm. on Tech., Comm. on Homeland & Nat’l Sec., Subcomm. on Biometrics, Biometrics Glossary 4 (2006), available at http://www.biometrics.gov/Documents/Glossary.pdf.
So disclaimer number two, I am only talking about these technologies within the context of using them for authentication of digital and multimedia evidence in legal proceedings. OK. Nothing that I say from this point on should be taken to undermine or in any way lower the quality of evidence that can come from various biometric modalities in investigative and forensic uses.

OK. First off, let’s just dispense with handwritten signatures right now. I think I’ve never seen studies or heard of studies that look at the persistence of signatures over a lifetime. But you’ve got to be about two years old before you can even hold something to sign with.

So admittedly, we’re not going to have infants authenticating evidence, but you’re not going to have a persistent signature over a lifetime. You would have to get handwriting exemplars from every person on the planet. It’s not going to happen.

It’s easy to use, certainly, but you can also spoof it when we’re dealing with a static condition. I’m not asking you or challenging you, but you could have gone onto Google two years ago and done a Google image search. OK. You type in the words, and say I want images related to this.

Well, two or three years ago, if you typed in my name, the first image that came up was a copy of my signature because it was on the FBI website as having signed a letter that was written to the community of imaging scientists. And so anybody could have just copied that photograph, cut and pasted it in.

I, along with two other chairs of scientific working groups, wrote a letter to the National Commission on Forensic Science. Rather than physically sign a copy of the document, I just sent him my signature, and he pasted it into the document because the document said what I wanted it to say. So signatures, they’re not an adequate means of biometric authentication.

DNA certainly is persistent over a lifetime. You can individualize to over seven billion people.

In an earlier version of this slide, I had the twins, “?” Monozygotic twins do have identical DNA within the twenty-six markers that are used in criminal justice systems or however many they have in Europe. But once you begin to look at the full DNA signature, the entire string, it is possible to individualize every single person. There are no systems, though, that do that on a regular basis. And it’s not used for criminal justice purposes.

The biggest problems with using DNA for authentication, certainly, is that it’s costly and slow. Although we now have DNA systems that are approaching one-hour turnaround time.

And the biggest problem that I see if we’re going to use a biometric in authenticating evidence is how are you going to get people to actually give their DNA. People aren’t comfortable taking their own buccal swabs. It’s hard to spoof. Absolutely, it’s hard to spoof. And by spoofing, I mean fake it. But not practical to employ for authentication.

Friction ridge. Certainly, persistent over a lifetime as studies have shown.
Friction ridge includes fingerprint, palm print. You could even extend it to sole pattern, sole prints, if you were interested in it. Yet we don’t have—the problem with fingerprint and the other biometrics that I’m going to quickly talk about is that they’re all exemplar-based. DNA is deterministic. All of these other biometric modalities are sampling-based so that it’s all done based on similarity between the samples that you have examined up to that point.

So to really say that every person on earth has a different fingerprint pattern at this point in time, we would have to sample every one of them.

Now, having said that, the FBI ten-print fingerprint systems can be run very effectively in what’s called a lights-out mode where the ten-print fingerprints allow you to quickly return back to the field in identification without ever having a human being involved in that process.

It’s easy to use. If any of you have been to Disney recently, they use a fingerprint system that is linked to your card or your—they’re now going to RFID wristbands. You scan your finger, you get into the door.

PROFESSOR CAPRA: iPhones now.
MR. VORDER BRUEGGE: iPhones, that’s right. It’s hard to spoof. You can certainly—there have been instances of people altering their fingerprints to try and avoid detection. There’s a lot of literature out there about faking fingerprints. But given certain liveness testing that can be used, it makes it very difficult to spoof it.

I’ve merged face and iris. Face, as much as I spend my life now working with face recognition, it is a very difficult thing to deal with over a long period of time or even a short period of time.

We’ve all heard the stories about driver’s license bureaus saying, “Don’t smile when we take your photograph.” It’s because a comparison of my face between me being neutral and me smiling is a reduction in the match. It actually ends up that smiling to smiling has better performance than neutral to neutral because smiling makes you more unique, but we can talk about that over a beer.

When you think about it, if someone gets arrested, what’s the likelihood you’re going to get them to say, smile.

MR. JOSEPH: Tom DeLay.

MR. VORDER BRUEGGE: That’s right. Tom DeLay, yes, he did that. As with the other, there’s no biological background that makes it deterministic for face recognition, so we need to sample everybody if we’re going to individualize. It’s certainly easy to use.


There are apps you can get and put on your phone that will unlock the phone with through face recognition. So you can use face recognition to unlock your mobile phone.

Big problem, it’s not private. Everybody who goes out in public, you can get their photograph, you know. This Google Glass idea is a major concern for a lot of people for a lot of reasons. But one of them being the privacy issue.

And actually, if I could riff just briefly, consider the relationship of anonymity and privacy. The public—being out in public space, the point is you’re anonymous. It’s when you can attach name and biographic information to that face or person that makes it a privacy issue.

Iris recognition; there is a highly accurate way of sampling the iris pattern. It’s done in the infrared so it’s not as easy to spoof, but if you have a device, if you have an infrared camera out in public, you could take pictures of people’s irises. There are systems that can pick up iris and do matching as you walk through something like a metal detector.

So that makes it easy to use. There’s no physical contact like a fingerprint. It’s just electromagnetic radiation.

There is some debate about the persistence of the iris signature over time. There’s a real heavy-duty argument going on. But it has been shown to work in large systems.

The government of India is biometrically enrolling every one of their citizens for the purpose of providing social services. They’re using finger, face, and iris. And those are being used together. You’ve got a lot of instances of people that are missing digits or they don’t have eyes. So with the multifactor authentication, they’ve got a lot of backup there.

Regardless of what we say here today about biometrics, there’s going to be a lot of challenges. At the moment I’m unaware of any biometric systems that are used for authenticating evidence. As I’ve already stomped on handwriting enough, I’ll move on.

It’s my personal opinion that friction ridge and iris are probably your best options from usability standpoint and accuracy standpoint. But test and evaluation is going to be critical for any of these things.

There is a big problem in getting from research and development into production. There are going to be problems with systems, and you can’t just expect to buy something off the shelf and put it in.

118. See Keith Wagstaff, Unlock Your iPhone with Your Face, TIME (Jan. 10, 2012), http://techland.time.com/2012/01/10/unlock-your-iphone-with-your-face/.


Finally, coming back to the idea of binary hashing to ensure integrity, you could then implement the biometric template, this digital file that represents your iris or your fingerprint signature and attach it to the data that is of interest actively and then wrap it in some way to make sure that it is further authenticated or the integrity of that is maintained.

MR. HARIED: Richard, if you took a biometric, whether it’s fingerprint or iris and combined it with a pin code to the user who had the input to a system, would that increase the reliability of that system?

MR. VORDER BRUEGGE: Yes. Anything that you could do to—well, it would increase the reliability for not being spoofed. Yes. So any multifactor approach that you take is going to increase the accuracy of the system.

Reliability is a question of how much complexity an additional factor is going to add in and the chances for pieces to be inserted, ways for people to get in and game the system.

I mean, people that have biometric access controls for their garages or their homes, there’s nothing stopping a person from just pulling the sensor off and cutting the wiring back. Physical approaches can always come up.

V. HEARSAY

PROFESSOR CAPRA: Now we’re going to move to the area of challenges presented by electronic evidence with respect to the hearsay rule and its exceptions. And we start off with Professor Jeff Bellin on eHearsay.

PROFESSOR BELLIN: Thanks to Dan and the Committee for having me here. This is my favorite topic, so I’m happy to be able to address the group.122

I don’t usually point this out, but for these purposes, I wanted to highlight my Twitter handle so that you understand that I know what I’m talking about. There you go.123 You can follow me on Twitter.

The way this started for me was a couple years ago, I started thinking about the phenomenon of texting and social media. If you’re like I am, a professor, you’re engaged with the younger generation, you see that it’s really taking over the way that they communicate.

I tried to think about this phenomenon as a flood of new information that’s going to be available to the litigation system and how we might want to handle it.

I agree with an earlier comment that it’s not just that the technology has changed; I think that would be significant by itself, but the change runs in parallel with a norm change in how we communicate. And those two things together are what create the need, the potential need for change.

The way I looked at it was, there’s a lot of positive characteristics of this communication in terms of its use for the court system—for example, the comments that people are making in social media and text messages.

122. For Professor Bellin’s PowerPoint presentation, see Appendix V.
They’re comments about things that they recently perceived. So there’s not a significant problem with memory.

Generally, the way that people use these tools, they communicate with friends and family, and so there’s some sense that they would be somewhat reliable when they do that.

Then this, I think, is one of the biggest pieces of reliability—the communications are frozen in time in a way that other types of communications generally aren’t.

Not only do we have the substance of the communication, but we also have information about it, like the precise time and date that it was sent, the recipient, and who sent it.

Unlike a lot of other communications, this information about a text or similar communication can be verified multiple ways. You have it on the sender’s phone, on the receiver’s phone. Then through the servers and things the message passes through, you can subpoena AT&T and find out was there really a text message with this content sent on this day, et cetera, which you couldn’t do with just an overheard oral comment.

So to me, the development of text messaging and similar communications creates the potential for the court system to overcome what I see as one of the biggest problems we have, which is that, although we celebrate it, live witness testimony has a couple of big problems that I’ll just flag.

One is, people forget over time. Trials are generally a far distance from the actual events that they’re about. And then the other big one is that people don’t want to cooperate. They don’t want to testify.

So a lot of the people who have valuable information are not going to share it, either because they can’t or because they’re uninterested in sharing. And then obviously, you have all the issues of people shading their testimony in court.

Let’s think about this problem or potential boon for the court system. Obviously the big problem here is that these are all out-of-court statements. If you want to use them, you have to create some kind of hearsay exception. And if you wanted to do that, what characteristics would you require to try and capture what’s good about these communications?

Here are the things that I thought about. One, you might cabin this to recent descriptions of events. I think a big factor in reliability is that text messages and social media posts generally arise prior to the controversy and so that makes them seem reliable. So you might want to require that.

What I think is a big plus here is you could just require that if someone wants to offer one of these, they offer the actual communication, not testimony about it. So you could require that it be recorded.

Notice you’re not really losing much with these so far because this is the normal pattern, particularly, of text messages.

And then finally, you can make it apply only if the declarant is unavailable or, conversely, if the declarant testifies. If the declarant testifies, then a lot of the objections to allowing hearsay go away anyway.
But certainly if the declarant’s unavailable, then what you’re talking about is the hearsay versus nothing at all. And I think then the argument for the hearsay becomes much stronger.

As I went through this, what I realized was, these things that you might want in a hearsay exception actually are pretty similar to a hearsay exception that was proposed in the 1960s—the statement of recent perception exception.\(^\text{124}\) And that proposal actually has a long pedigree as well.

You can see from the history of evidence rulemaking that the recent perceptions exception is not something that I just created out of whole cloth. I really did draw from the historical analogues of the exception.\(^\text{125}\) If you go all the way back to 1896, James Bradley Thayer proposed an exception.\(^\text{126}\) That’s the beginning.

And you can see that basically, what I was talking about, the historical analogue that’s most directly related is the statement of recent perception.\(^\text{127}\) That was proposed as Federal Rule of Evidence 804(b)(2) by the Advisory Committee in the 1960s and was ultimately rejected by Congress.

But basically, the hearsay exception that I propose, I think, does capture all the beneficial qualities of these electronic communications, is modeled on and uses a lot of the same language from the statement of recent perception exception, except that because I really like the recorded piece of it, I went back to Thayer’s proposal, which required a writing and built that into the rule that I was proposing because I think that does make these statements much more reliable. And then making the same exception applicable if the person testifies, from the Uniform Rules.

So while the proposal seems like a very new proposal, it actually just builds on the proposals that came before from evidence luminaries of those times. And because of the change in the communication norm and technology, it’s actually much more relevant now. In a way, these exceptions suddenly make a lot more sense in light of what we can use them for given the changing communication norm.

I have an article out there that was circulated to the Committee, providing a more thorough justification and explaining why the particular language is important.\(^\text{128}\)

But I think the best way to show how it would work is to use a couple examples from cases. I looked through the case law and found cases where someone’s offering text messages or social media posts and tested them against the rule that I propose.

Here’s one from a federal case out of the Third Circuit.\(^\text{129}\) The defendant was on trial for bribing a juror. And the juror who testified in the case had

---

125. See app. V.
127. See app. V.
sent a text message to her sister. After the person had tried to bribe her, the juror went into her home like a lot of us would have and told people, “Hey, this strange thing happened.” She sent a text to her sister, and it says, basically, “Someone just came over and tried to bribe me in this case. And that’s why I didn’t want to be a juror in the first place.”

Let’s talk about how this statement would fare under the proposed exception. Notably, in the Blackett case, it was allowed in as a past recollection recorded, which is just an incorrect application of that rule because the witness remembered. This serves as a counterexample, by the way, to any response that text messages and the like can be handled by the existing evidence rules; they’re handled in a way that distorts the existing rules.

Now if we use my proposal, you’ll see that it fits all the requirements. It’s recorded. It has to be a communication, which it is. It has to go from one person to an intended recipient. It satisfies that. (Recall the exception is actually two pieces. This is illustrating one piece where the declarant testifies.) It had to be recently perceived. Then there’s some nits. It can’t be in contemplation of litigation. The main point here is to kind of keep out statements to police officers or elicited by police officers. The juror’s statement wouldn’t be disqualified on that ground.

I added another limitation in lieu of the language in some of the earlier iterations, that the statement had to be in “good faith.” I don’t like the good faith language because it’s too amorphous, and I don’t see how a judge can really tell.

I modernized the good faith limitation and provide that it can’t be anonymous.

This is an example of a text message that any rational system of evidence would allow in; it comes in neatly under my rule without any difficult interpretation.

Here is another example to illustrate the other piece of the rule, Rule 804(b)(5). This is basically the same exact exception, but this one would apply if the declarant is unavailable.

The example is a murder prosecution, and the defendant was the husband of a woman who sent this text message to her friend shortly before she was killed. The text message basically says that my husband is threatening me. He said he was planning to attend a funeral and not his funeral.

This was allowed in under the Iowa version of the residual exception. And what the Iowa Appeals Court said was that it fits the residual exception

---

130. See id. at 742.
132. IOWA R. EVID. 5.807 (“A statement not specifically covered by any of the exceptions in rules 5.803 or 5.804 but having equivalent circumstantial guarantees of trustworthiness is not excluded by the hearsay rule if the court determines that (A) the statement is offered as evidence of a material fact; (B) the statement is more probative on the point for which it is offered than any other evidence which the proponent can procure through reasonable efforts;
because it’s recorded, and juries can look at it for themselves. Note that that applies to every text message in the world. So if that’s a proper interpretation of the residual exception, then get ready for some exciting evidence rulings.

Again, if we apply my exception here, it’s a recorded communication, a text to the sister. Declarant is unavailable under this piece of the rule. Recently perceived event, not in contemplation of litigation. Not an anonymous statement. So this would be admissible under Rule 804(b)(5)—

PROFESSOR CAPRA: How do you know that it’s not in contemplation of litigation?

PROFESSOR BELLIN: Good question. It’s like all the evidence rules. It would just be from the context of the statement, you decide by a preponderance of the evidence, is this in contemplation of litigation?

Now this language I took from the previous rule, but the best way to interpret this, and I talk about this in the eHearsay article, is to track the language in Bryant about what is testimonial—whether the primary motive for making the statement is to use it in a prosecution. If it’s nontestimonial, basically, not an out-of-court substitute for in-court testimony, then it would fit.

And so you’d have this parallel where if it’s allowed under the Confrontation Clause, it would also be allowed under the hearsay rule.

JUDGE WESLEY: So if there were an order of protection protecting her, then it would not be admissible?

PROFESSOR BELLIN: Well, then it would change. The analysis would change, or like a custody dispute. And then you’d have an argument and again, like in the Bryant analysis, I would think of it as a primary purpose for the litigation as opposed to just there’s a mere prospect of litigation—because there’s in these cases always a prospect of litigation if you’re describing any kind of criminal conduct.

As I talk about in the article, this Rule 804(b) statement of recent perception exception was adopted in four states, although it didn’t make it into the Federal Rules. So part of what I do is draw from that case law; it’s not a lot because it’s states like Hawaii and Wyoming that don’t have a lot of case law. But what they do in those cases, they interpret it pretty narrowly so that there really has to be some sense that you’re making the statement for the litigation, not just that there’s litigation in the air.

The main reason to include this language—and I think it’s a good one—it gets you out from under the Confrontation Clause. And I do think there

and (C) the general purposes of these rules and the interests of justice will best be served by admission of the statement into evidence. . . .”).

133. Petersen, 2013 Iowa App. LEXIS 582, at *2–3.
136. See id. at 34 n.110 (explaining how Hawaii adopted the rule verbatim, while Wyoming adopted the rule for civil cases only).
137. See id. at 41–46 & n.147.
would be a lot of resistance to this rule if a statement to the police or something like that on the police Facebook page could come in. That’s what this is trying to keep out. Both if the police officer solicits the statement or you make the statement to the prosecuting agent, this piece of the exception is supposed to keep it out.

Just a couple kind of quick points, because I know there will be more discussion of it, about the way I drafted the rule. Because it’s targeting this electronic communication norm, I thought about trying to say that in the rule. And as I did, I realized it’s almost impossible to define “electronic” in a coherent way. And then you see that none of the other hearsay rules does this; none tries to limit the rule to a particular medium of communication. So what I did is, I left it nonspecific. The rule would apply to anything: written statements, like a postcard as well.

I think it wouldn’t cover a lot of those. And, in retrospect, there is a benefit in that it makes the rule more broad and it can apply to any new technology that comes in the future.

It makes the rule work on some things from the past like postcards. But what it really does is, it opens it up so that, as everyone’s talking about, as the communication technology changes, the rule will still apply. I think that’s a positive.

Then the last thing—actually, two things now until Dan makes me stop. We talked about the prospect, and I think it was a good point Judge Woodcock made: what we don’t want is another Innocence Project where we’re saying, oh, these things that came in—now, he’s talking about photos but you might also say it about text messages—they weren’t valid and so this person was actually innocent.

But I want to highlight in that respect, the reason this idea frightens us so much is we currently have Innocence Projects because of the failings of live testimony. So it’s not a question of: Is this evidence unimpeachable, unassailable? It’s a question of: Would this help juries beyond what we’re already giving them, and we’re already running into some problems with what we’re already giving them.

My view is that this would help. And I think of it as I said at the outset; there’s a lot of information coming to the court system. One way to react to that is hunker down and hope that the things we have in place, the levees and the channels we already have will be able to handle the flood. And you know, they might.

Like I said, the rules will be distorted probably somewhat as judges struggle because the levees and channels we created weren’t in anticipation of this kind of flood.

But the big distinction between this and a flood is that this is our river. We made these rules. And so we can change the rules, and we can say, “Here’s all this information coming into an imperfect court system. Why not channel the information to where it’s needed and let the less valuable information go out to sea?”

PROFESSOR CAPRA: Thanks, Jeff. I’d like to ask Paul Shechtman for his thoughts on this possible amendment.
MR. SHECHTMAN: I should start off by saying that I don’t have a Twitter handle, and I’m not even sure I can use PowerPoint, but we’re going to try.138

Professor Bellin has titled his paper, eHearsay.139 And what I hope to show is that it’s really less about “e,” which is to say less about electronic evidence, than it is about hearsay. And that it addresses two questions that evidence law reformers grappled with throughout the twentieth century.

The first is: Should the law admit more hearsay from unavailable declarants? And the second is: Should the law admit more hearsay when the declarant testifies and is subject to cross-examination?

I start with unavailable declarants. This is to say we are talking about: Should we allow in more hearsay from people who are unavailable?

And the first proposal, influenced by Bentham, is that of Thayer.140 And Thayer required unavailability. He actually limited it to the declarant must be deceased. He didn’t limit it to recent perceptions. He required it to be written. He had something about not in the shadow of litigation, not in contemplation of litigation. And he didn’t require good faith.

Two years later—and this shows the influence of Thayer. This shows that scholars were more influential in his day than ours. Two years later, Massachusetts adopted an exception, which it still has. And it required unavailability like Thayer. It limited it to the declarant being deceased. It required recent perception. It said written and oral, a change that Thayer approved. And it had a contemplation of litigation requirement and a good faith requirement.

I’ll skip down. The broadest unavailable exception was the Model Code of Evidence.141 This was Morgan. This was rejected in every state in the country. And it simply required unavailability, written and oral, period. If he was unavailable, it came in.

And I’ll pause just to say one thing because this is an important point when it comes back to talking about Jeff’s proposal. Here is something from Morgan and Wigmore talking about should it be written or oral? Should it be both?

And what Wigmore and Morgan wrote in a book published in 1927 is that oral should come in because “the oath and cross-examination are everywhere considered sufficient safeguards against inaccuracy and perjury in reporting verbal as well as non-verbal acts.”142

So their view was that oral statements should come in. After all, the witness who is reporting them is in the courtroom subject to cross-examination. And I would—it’s not fair to Jeff, but where it says everywhere considered, you should know everywhere considered but except

---

138. For Mr. Shechtman’s presentation, see Appendix VI.
139. Bellin, supra note 124.
140. See Thayer, supra note 126, at 521.
141. MODEL CODE OF EVIDENCE (1942).
in Jeff's article because he makes that distinction that was the original Thayer distinction.

PROFESSOR BELLIN: They didn’t have a copy of my piece at the time.

MR. SHECHTMAN: If you go down—as Jeff points out, if you go down to the proposed rule, it had unavailability. It had recent perception. It was written and oral. It had the same contemplation of litigation, and it had a good faith exception.

Jeff’s proposal has it that the witness has to be unavailable. Although he would also do it for—and I’ll come back to this—if the witness has testified. It’s recent perception. It’s written. He adds it has to be limited to communications. I’ll come back to that.

He doesn’t allow the exception to reach oral communications. And he bars statements made in the shadow of litigation. He does not have a good faith limitation, but he uniquely has the requirement that it can’t be anonymous.

So that’s the legal history here, and it’s important, I think, because it sort of takes us away from eHearsay and asks more generally about evidence reform regarding hearsay statements from unavailable declarants.

I am now presenting a series of hypotheticals to test the application of Jeff’s proposed exception.143

So our first one is this. A text message from V to a close friend the day before the murder. “D hit me yesterday and threatened to return and ‘finish the job.’” It’s the day before the murder. It’s not going to be admissible under current rules. But it is under Jeff’s.

A voicemail message left by V on F’s phone, same as above. Right. The answer to that is that’s admissible under Jeff’s proposal, which is why Jeff’s proposal really isn’t an eHearsay exception. It picks up, as he points out, the postcard, and it also picks up the voicemail.

An oral statement from V to F, but otherwise the same. The answer is: that’s inadmissible under current law. It’s inadmissible under Jeff’s proposal because it’s oral. But appreciate that what we are saying is the person we’re not trusting is the in-court witness in that situation. And maybe that should be, but that’s the reason for the distinction here.

Let’s see. Same hypothetical, but F takes and maintains contemporaneous notes of V’s statement. Those contemporaneous notes don’t matter. It has to be the declarant who is doing the writing, the recording. It has to be that I am recording it.

MR. JOSEPH: Present sense impression.

MR. SHECHTMAN: All of these are the next day. Right. So none of them is a present sense impression.

MR. JOSEPH: Somebody’s taking notes.

MR. SHECHTMAN: It doesn’t matter.

MR. JOSEPH: The notes are a present sense impression.

143. See Appendix VI for these hypotheticals.
MR. SHECHTMAN: Of that person, but not of the out-of-court person who made the statement about what happened to him the day before. So you’re not getting that in under current hearsay rules. And you’re not getting it in under Jeff’s proposal.

The next is a diary entry made by V. That is recorded. But that’s not coming in under Jeff’s proposal because if you look at the top, he’s got a communication requirement. And that is not a communication.

Now, that’s—for those of you who teach evidence, that’s an odd twist because what we usually say is, when something is intended as an assertion, it is more unreliable. Because you’re communicating it to another person, and there’s a sincerity issue. But for Jeff, the communication makes it more reliable and so the diary stays out.

The next one is same as above, but with the addition, “If anything happens to me, give this text to the police.”

I don’t know the answer to that. It may be in contemplation of litigation. There may be a Crawford problem, but you’ve got issues as to what is meant by contemplation of litigation.

The next is the same. And this is Judge Wesley’s point, the same as (1), but V and D are engaged in a bitter custody dispute. Is that in contemplation of litigation? What litigation does it have to be?

The next, an anonymous note to V’s mother, “I was present yesterday when D hit V. She needs protection. I can’t disclose my identity. Too scared.” The answer is that’s inadmissible because it’s anonymous, and that takes it out.

Now, then I changed it, same hypothetical, but the identity of the texter can be determined, and he’s now dead. He’s unavailable.

But I think, if I understand Jeff’s rule right, it is, was the texter intending to be anonymous, not can we figure out who he was. So the principle seems to be unless you own it, we won’t admit it. And that may make sense, but it’s odd to me as well, why anonymity is a requirement of this rule.

So that’s the first part of this rule. And there are lots of twists in it that I’m not sure make sense in terms of communicative, anonymous, and the like.

The second part is the issue that we now have a testifying witness.

Now, here the history, as some of you will recall, is this: when the Federal Rules were authored—and I’m going to talk about inconsistent statements, not consistent statements. The reason for that is, we’re letting in—particularly with our proposed amendment to Rule 801(d)(1)(B),144 everything that’s consistent that’s useful is coming in. And so one doesn’t really need a reform effort there, but inconsistent statements, you might.

And when the rule on prior inconsistent statements was first proposed, it said such statements were admissible if “the declarant testifies at the trial or

---

144. The proposed amendment to Rule 801(d)(1)(B), scheduled to take effect December 1, 2014, provides that a prior consistent statement is admissible for its truth whenever it is properly admitted to rehabilitate a witness’s credibility. See FED. R. EVID. 801(d)(1)(B).
hearing subject to cross-examination”; which is to say, as an in-court witness, and it’s inconsistent with his testimony. That was the proposal.

And the history here is that Sam Ervin, alone, took the position when the rules reached Congress, that the proposal was problematic because you could convict somebody without an in-court accuser.

So what you have is, your star witness for the prosecution says, “The defendant did it.” Now you come to trial, and he says, “Dan Capra did it.” Can I put in his statement to the police in which he said the defendant did it? That is an inconsistent statement. The defendant has testified.

And Ervin said, “We’re going to convict people—it’s substantive evidence, after all. We’re going to convict people with no in-court accuser.” And so the compromise was to say that inconsistent statements are admissible as substantive evidence only when made at a formal proceeding under penalty of perjury.

And that is why a prosecutor, a federal prosecutor who is concerned about his witness turning, will put him in the grand jury and lock him in because now I’m under oath at a proceeding, and that testimony comes in substantively.

Now, what Jeff proposes is a halfway house between the two. The halfway house being the same rule that he has for unavailable witnesses.

And so one might begin by asking the question: I have two very different problems. My first problem is: Should I let in more hearsay from unavailable declarants? My second problem is: Should I let it in substantively? Because remember, all these things are coming in to impeach. Should I let in substantively more testimony from in-court witnesses? Those are very different problems.

And so it surprises me that the answer to those two problems are the same, which they are under Jeff’s proposal. Because he simply takes his unavailability exception, and he applies it where there’s an in-court witness.

And let me show you what I mean by my being surprised. Let’s assume that we have an anonymous message. Now, our witness is testifying. We’ve now figured out who he is. Right. He wrote it anonymously, but we know who he is. And he is the person on the witness stand. And he says, “That’s my anonymous message.”

But he changes. He no longer says the defendant did it. He says Dan Capra did it. Right. Under Jeff’s rule, that’s inadmissible because his same condition that it be anonymous applies in both situations.

Take the diary. Now I have the situation with the diary, and the answer is: it’s inadmissible if he’s unavailable, but it’s also inadmissible if he’s on the witness stand. So he changes his testimony. In court he says one thing. In the diary, he said something else. The answer is: the diary is inadmissible because it’s not communicative.

Finally, the whole notion of oral and recorded. So now assume it is oral. It is inadmissible—it is oral to the police. And to the police, he says the defendant did it. Turncoat on the witness stand. He says Dan Capra did it.
The answer is, under Jeff’s proposal, that is inadmissible because it’s oral. And the reason for that is, we were concerned about it being oral. It requires an in-court witness to know it’s true. But assume the fella says, “Yes, that is what I told the police.” Now we know he said it. And the question is: Why are we still keeping it out?

And Jeff is keeping it out because it’s oral; even though we know it was made because the witness has acknowledged it.

So for me, that’s a long way of saying, it may well be that there should be hearsay reform. It may well be that the Advisory Committee got it right with unavailable witnesses, and there should be a broader exception.

It may well be that the Advisory Committee got it right with testifying witnesses, and there should be a broader exception.

But I would think about this more as hearsay and less as “e.”

PROFESSOR CAPRA: Thanks, Paul. We give a right of reply. We’re running long, but you get a short right of reply.

PROFESSOR BELLIN: I enjoyed that a great deal. This is what I would say: I would look forward to your presentations critiquing the other hearsay exceptions, because I think my proposal would actually seem stronger. I can’t imagine what you would say, for example, about the present sense impression exception.

I mean, they’re all going to be over- and under-inclusive, right? What Paul’s pointed out is there would be some statements that you might have wanted in or out under a different rule. And maybe I could have accommodated that by putting in a good faith or similar requirement.

I just didn’t like that because what I wanted to accomplish was to make it clear. I think that’s part of what you illustrated; there is some clarity in the application of this rule, and so judges will be able to apply it consistently. It also will exclude some things that you might want in—or let in things that you might not want, but that’s the case with all the hearsay exceptions.

Especially if you think about the Rule 804 exceptions, such as statement against interest or dying declarations. Everyone acknowledges that the statements that come in under these exceptions may not be reliable. But we think it’s better than just doing without any statement coming from the unavailable declarant.

Finally, I didn’t have the idea this proposal would just be accepted as is or you can’t use it. I’d be happy for people to suggest changes. I just think there is all this new information out there, and we don’t have a way to analyze it under the current exceptions. This was my suggestion, but I’m sure there’s other ways to do it as well.

PROFESSOR CAPRA: Thanks.

MR. SHECHTMAN: I’ll say one thing because it was criticism, but what is so good about Jeff’s paper is, he takes us back to two rules that were proposed by the Advisory Committee that have been forgotten. Which is to say, that the original proposal for recent perception and a much broader proposal for testifying witnesses, they are basically lost to history.
And the good thing about the paper is, it brings them back to life and asks, “Should we have broader exceptions for both?” And that’s a very good thing to be talking about.

PROFESSOR CAPRA: With regard to the proposal on testifying witnesses, there are several Standing Committee judges that have suggested that the Committee go farther and just say, “If you’re testifying, everything is admissible substantively.” So yes, this is within that trend. Greg.

MR. JOSEPH: I’ve been taking testimony for almost thirty-nine years. And all I find are people who under oath lie, misremember, misperceive, misstate, dissemble, color, shade. And the thought that you’re not going to be able to cross-examine this stuff and that you’re going to open the door more broadly to hearsay from unavailable declarants is horrifying.

Why would I assume that because they’ve put it in a tweet, they’re being more candid than somebody who is sworn to tell the truth?

MR. SHECHTMAN: I would just say the following: we have a lot of hearsay exceptions, like the coconspirator hearsay exception, because we believe people are more reliable out of court than in court.

So it’s not crazy to think about broadening this in the way that Jeff did. And many of these come very close to present sense impression.

The last thing I’ll say here is: one of the failings that all of us have as evidence scholars, those of us who teach evidence, is you have four states that have done this. And Massachusetts has done it for a very long time.

It’s not fashionable for law professors to say to their students, “Could you find out what’s happening in Minnesota?” But it would be interesting to see whether people in Minnesota or Hawaii or these other states think that the world has come to an end.

PROFESSOR CAPRA: Continuing our discussion of hearsay issues, Professor Deirdre Smith is going to speak to us about the Confrontation Clause and electronic evidence.

PROFESSOR SMITH: My remarks are going to very briefly address two questions: To what extent does the right to confrontation under the Sixth Amendment add a further barrier—beyond what we’ve already been talking about this morning—to the admissibility of electronic evidence? And the short answer to that is, “not much.”

And are there any unique or interesting questions about the intersection of the Sixth Amendment and electronic evidence? And the short answer is, “maybe a few.”

The first thing I want to do is refer everyone to Jeff’s excellent article that was published in the Texas Tech Law Review in 2012, Applying Crawford’s Confrontation Right in a Digital Age, which goes into far

---

145. See Bellin, supra note 124, at 34 n.110.
146. The Confrontation Clause provides: “In all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him . . . .” U.S. CONST. amend. VI.
more detail than I am this morning about this issue. And specifically, in light of my short answer, the “not much difference,” he makes some suggestions about directions that the courts may want to go.

Although the precise contours of the Supreme Court’s jurisprudence about the Confrontation Clause may be less than clear, I’ll make some observations this morning about the things that at least we’re pretty sure of as of right now.

Evidence offered by the government against a criminal defendant can potentially implicate the defendant’s rights under the Sixth Amendment when the evidence is, first of all, admissible hearsay. That is, it’s being offered for a hearsay purpose, but it meets a hearsay exception and—and this is where the action has been during the past ten years since Crawford v. Washington—if the statement can be properly characterized as being “testimonial.”

Categorization of admissible hearsay as either testimonial or not testimonial is the critical first step. If it does get past the hearsay barrier, most electronic evidence that would be offered by a prosecutor is likely to be classified as nontestimonial under that current conceptualization.

As we know, the Supreme Court has not set out exactly a precise framework for figuring out what’s testimonial and what isn’t, but from cases like Davis v. Washington and Michigan v. Bryant, it’s clear that a court has to examine the purpose of the statement and determine whether the declarant made the statement for use in a criminal prosecution to prove past events.

This “primary purpose” or “primary motive” test employs an objective standard. And without using up all of my time trying to offer my explanation of the various opinions in Williams v. Illinois, I will just say it appears that there are four Justices who think this test should be further refined to limit it to statements primarily made for use in a criminal prosecution of a specific, identifiable individual.

The various kinds of electronic evidence we’ve been talking about this morning fall along the testimonial spectrum under this approach. There are large categories of electronic evidence—a lot of what Jeff was just talking about—that would be highly useful to prosecutors, but are quite clearly nontestimonial based upon the Court’s current conceptualization of that distinction.

These would be emails, texts, tweets, direct messages between family, between friends, between business associates, coconspirators, and so forth, or social media posts, directed to no one in particular.

By and large, with the exception maybe of something that says, “Give this to the police if I end up dead,” these are not made for purposes of providing information about past events that would be used in a criminal prosecution. There may be plenty of hearsay and authentication issues with this kind of evidence, but there are not likely to be Confrontation Clause

149. 132 S. Ct. 2221 (2012).
issues. And, if some of the proposals this morning get passed, there may be even fewer hearsay issues.

And prosecutors, of course, may offer electronic evidence as part of a prosecution when criminals commit crimes online, when the criminal activity itself is in the form of electronic evidence or it’s captured in some electronic format. But by and large, such evidence generally does not implicate the hearsay rule and therefore, does not present any Confrontation Clause concerns.

When we get to statements to or by law enforcement officers, that’s where we’re a bit closer to the testimonial characterization at the end of the spectrum. Examples of this might include a statement from a complainant or other witness that’s in an electronic format when it’s communicated to law enforcement. For example, there are many police departments that now have “text tip” programs where you can send information to law enforcement to report criminal activity.

Now, to the extent that that text message is made to report ongoing criminal activity or to summon the assistance of law enforcement as part of an emergency, it’s really no different from dialing 911. And that’s really going to fall outside of that testimonial line that was drawn in Davis and Bryant.

There’s even a recent Eighth Circuit opinion, United States v. Brooks,150 that held that data reports from a GPS tracker attached to a suspect’s car were nontestimonial because their primary purpose was to locate the suspect.151 I have a question about whether they were hearsay, but putting that aside, they were found to be nontestimonial.

Statements to law enforcement outside of an ongoing emergency context are more likely to trigger confrontation rights, and police are making increased use of Facebook, Twitter, and so forth to collect information from the community from potential witnesses. But given the potential authentication problems with those, and, again, the hearsay problems, I suspect those communications, at least for the time being, will serve more of an investigative function than as substantive evidence at trial.

One area where there is some controversy concerns electronic evidence that’s potentially admissible under the business records exception of Rule 803(6).152 As we know, an increasing amount of regularly conducted activity is captured through electronic evidence, logs and ledgers, and so

---

150. 715 F.3d 1069 (8th Cir. 2013).
151. Id. at 1079–80.
152. Fed. R. Evid. 803(6) ("A record of an act, event, condition, opinion, or diagnosis if: (A) the record was made at or near the time by—or from information transmitted by—someone with knowledge; (B) the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether or not for profit; (C) making the record was a regular practice of that activity; (D) all these conditions are shown by the testimony of the custodian or another qualified witness, or by a certification that complies with Rule 902(11) or (12) or with a statute permitting certification; and (E) the opponent does not show that the source of information or the method or circumstances of preparation indicate a lack of trustworthiness.").
forth. And even when it’s in electronic form, courts have not had difficulty finding that that evidence fits within the business records exception.

If such evidence is offered against a criminal defendant, then the question becomes: Is it a testimonial business record that would trigger confrontation rights? The case law is fairly consistent that if the evidence fits squarely under all of the requirements of Rule 803(6), including the requirements of Rule 902(11) for certification, it’s going to place the statement outside of the testimonial category, and there is language in *Crawford* that suggested that that should be the case.

That trend is true for electronic evidence as well. So, for example, there are cases involving data reports of cell phone activity logged by a phone carrier, and courts have concluded that the carrier reports of such activity don’t implicate the Confrontation Clause. There’s a Tenth Circuit opinion, *United States v. Yeley-Davis*, that reached that holding.

However—and this is where it gets a little trickier—if it appears that the purpose behind the creation of electronic records involves a potential criminal prosecution, then the hearsay rule, as well as the Confrontation Clause, may foreclose admissibility.

In the majority opinion in *Melendez-Diaz*, if you remember, Justice Scalia indicated that he was very doubtful that the “business record” classification or “public record” classification could be appropriately applied to the chemist’s analysis of the drug in that particular case because the chemical analysis was run and the report was created in anticipation of a criminal prosecution. And that scenario implicates the “trustworthiness” concerns about such records, which would take the evidence outside of the exception pursuant to subsection (E) of 803(6). This is the same trustworthiness concern that was raised by the Supreme Court in the 1943 opinion in *Palmer v. Hoffman* where the Court held that the declarant’s regularly conducted business activity was the production of evidence for use at particular trials, which rendered the record inadmissible as a business record.

This suggests that there’s a very close alignment between the primary purpose test that has been developed under the Confrontation Clause jurisprudence and this trustworthiness concern that takes records created in anticipation of litigation outside of the business records exception.

But in the electronic evidence realm, discerning the primary purpose, either for this trustworthiness analysis or for Confrontation Clause purposes, can be a very challenging task for judges. And one example of where reasonable judicial minds can differ with respect to such purposes is

---


156. 318 U.S. 109 (1943).

157. *Id.* at 113–15.
an evidence question that arose in a child pornography case from right here in the District of Maine, *United States v. Cameron*.

Now, the case—or what’s left of it—is still pending before Judge Woodcock, so it’s not one we’re going to discuss in any depth here.

PROFESSOR CAPRA: We can say the First Circuit wrongly decided this, though? Can’t we say that?

PROFESSOR SMITH: I’m about to get there, Dan. Exactly. But I have to mention it because it’s such an interesting case. And I’m also going to give a very oversimplified description of what was a very complex opinion.

So as I mentioned, it’s a child pornography case. And at trial, the government offered a range of electronic evidence to prove that the defendant had received and possessed child pornography on his home computer. The activity was proven in part through tools that were regularly used by internet service providers, and much of the evidence from the ISPs was very easily classified under Rule 803(6) as being business records.

However, on appeal, a divided opinion of the First Circuit held that some of the evidence implicated the defendant’s confrontation rights. The evidence the majority found problematic were reports that were created by Yahoo! employees setting forth the IP address, screen names, and some of the images that they had captured about a specific user. They didn’t have a name, but they identified a specific user. The reports were turned over to law enforcement. The majority concluded that these reports were created by Yahoo! for the “primary purpose of establishing or proving past events potentially relevant to a later criminal prosecution.”

So there was really a two-to-two tie vote, I would say, on the issue. In this case, we have Judge Woodcock at trial (who, I would add, issued his ruling prior to the *Bryant* opinion), and Circuit Judge Howard in dissent concluding that the reports were business records and nontestimonial based upon their primary purpose.

The two judges in the majority concluded not only that the reports were testimonial, but they also commented that the reports were akin to the evidence at issue in *Palmer v. Hoffman*. And they suggested the records may not clear the hearsay barrier to admissibility in addition to implicating the defendant’s confrontation rights. So they drew a distinction between records created pursuant to a business practice and for a business purpose, and held that the latter controlled the issue of whether they were testimonial.

---

159.  Id. at 189–91.
161.  Id. at 643–49 (quoting Bullcoming v. New Mexico, 131 S. Ct. 2705, 2714 n.6 (2011)).
162.  Id. at 646.
163.  Id. at 648–49.
164.  See id. at 648.
What I found remarkable about this case is that arriving at these conclusions required these judges to delve very deeply into the technology behind, first, the data capture that was done by the internet service provider, and second, the creation of the reports. It is very dense reading, both the majority and the dissenting opinions, as well as Judge Woodcock’s ruling.

Therefore, I think the primary significance of electronic evidence with respect to Sixth Amendment questions, particularly in the context of records of a regularly conducted activity, is the challenge for litigants and for judges to discern that primary purpose.

And it will be very interesting to see how this case law develops, particularly in the context of child pornography and other types of crimes where the criminal activity and the investigations are very largely happening in electronic form.

So, in short, as I mentioned, is there anything really unique or special about electronic evidence in the Confrontation Clause realm? Overall, other than a few interesting questions and some particular challenges, I would say “probably not.”

PROFESSOR CAPRA: So there was a recent case from a circuit court, United States v. Keita.165 It involved records kept by American Express, called point-of-contact reports.

And these point-of-contact reports are reports about apparent fraud. And American Express uses those reports to decide whether to send them over to law enforcement. And yet the court found no primary motivation, so they were not testimonial.166 Really what they were trying to do is to get their money back and trying to make sure it doesn’t occur again. So the issue of motivation of business-type electronic records is challenging and courts have different views.

PROFESSOR SMITH: And I think part of the context here is that there’s the whole statutory mechanism behind the child pornography laws that impose mandatory reporting requirements on the ISPs and so forth. So I think that backdrop contributes significantly.

MR. SHECHTMAN: I take it in the case where Judge Woodcock got it right, you could get that into evidence, right? You just have to call the person who made that report to put it all in. It can all get before the jury?

PROFESSOR SMITH: Right. So the issue was—and Judge Woodcock can correct me where I’m wrong—but the issue was who was called to get those in. There were witnesses from Yahoo! who were explaining the process. It was just not the specific individual who had created the reports.

PROFESSOR CAPRA: So you’d have to call the person who prepared the report if you could ever find that person.

PROFESSOR SMITH: Right. So there was a description of the process and how it happened.

MR. SHECHTMAN: Or presumably recreate them if the database was still there.

165. 742 F.3d 184 (4th Cir. 2014).
166. Id. at 190.
JUDGE GRIMM: Right.

PROFESSOR SMITH: That’s interesting.

JUDGE GRIMM: Have the raw data and do it from that.

PROFESSOR CAPRA: It’s like redoing a forensic test if the analyst who did the first one is not available.

VI. ELECTRONIC EVIDENCE AND DISCOVERY

PROFESSOR CAPRA: Alright. The next topic is about an issue, that arises in the area of relevance, and it is created by problems in managing and producing electronic evidence. So what we have here is an interface between electronic discovery issues and evidence issues, and Judge Scheindlin will take us through that.

JUDGE SCHEINDLIN: I’ve divided my talk, and it is a rather formal talk, into four parts. First, I want to say that Professor Capra suggested and approved this topic because we’re going back to the past when we talk about adverse inferences. They are very, very old. I want to first deconstruct the adverse inference; what is its purpose, what are the possible purposes?

Then I want to address the adverse inference as an evidentiary tool, which is not something the civil rule is focusing on, the evidence part of it.

Then I want to very briefly touch on the new proposed Rule 37(e), which is only a week or two old. Those of you who spent the last one or two

---

167. For Judge Scheindlin’s PowerPoint presentation, see Appendix VII.

168. Editor’s Note: Judge Scheindlin’s analysis is directed toward the then-extant version of the amendment to Rule 37 that the Civil Rules Committee had revised after public comment. The Civil Rules Committee subsequently made several substantial changes to the proposal. The changed proposal was approved by the Standing Committee and the Judicial Conference and at this writing it is being considered by the Supreme Court. The proposal analyzed by Judge Scheindlin at the symposium provided as follows:

(e) If a party failed to preserve electronically stored information that should have been preserved in the anticipation or conduct of litigation, the court may:

(1) Order measures no greater than necessary to cure the loss of information, including permitting additional discovery; requiring the party to produce information that would otherwise not be reasonably accessible; and ordering the party to pay the reasonable expenses caused by the loss, including attorney’s fees.

(2) Upon a finding of prejudice to another party from loss of the information, order measures no greater than necessary to cure the prejudice.

(3) Only upon a finding that the party acted with the intent to deprive another party of the information’s use in the litigation: (A) presume that the lost information was unfavorable to the party; (B) instruct the jury that it may or must presume the information was unfavorable to the party; or (C) dismiss the action or enter a default judgment.

(4) In applying Rule 37(e), the court should consider all relevant factors, including: (A) the extent to which the party was on notice that litigation was likely and that the information would be relevant; (B) the reasonableness of the party’s efforts to preserve the information; (C) the proportionality of the preservation efforts to any anticipated or ongoing litigation; and (D) whether, after commencement of the action, the party timely sought the court’s guidance on any unresolved disputes about preserving discoverable information.

See app. VII. For Judge Scheindlin’s evaluation of the altered proposal currently before the Supreme Court, see her article included in this issue. Shira A. Scheindlin & Natalie M. Orr,
years thinking about the word “willful” can forget about it. Willful is not in the new proposal. It’s been rewritten. And I’m going to show you the rewritten proposal.

Then finally, like a lot of the speakers here, I, too, wrote a rule of evidence. Why not write a rule once in your lifetime?

Let me start with this business about deconstructing the adverse inference. There’s no debate that Rule 37, in particular, is meant to serve the purposes of deterrence and punishment. That’s fairly obvious. There’s an entire body of case law that has developed around the use of the adverse inference as a sanction to deter people from doing it or punish them for doing it. 169

And this body of law has become marked by a disarray of circuit opinions regarding the level of culpability; that is, the state of mind of the spoliator that is needed to support the imposition of the adverse inference.

And the circuit split is deep. There’s some things the circuits agree on. They agree that before an adverse inference can be imposed as a sanction, the moving party must show that the lost or destroyed evidence was relevant, the evidence was in the control of the spoliating party, and that party had a duty to preserve the lost evidence. 170 But that’s where the agreement ends.

The courts continue to disagree as to the level of mental culpability by the spoliating party that would permit the court to give an adverse inference instruction. Half of the circuits require bad faith. 171 “I intended to deprive


170. See, e.g., Stocker v. United States, 705 F.3d 225, 235 (6th Cir. 2013); Vulcan Materials Co. v. Massiah, 645 F.3d 249, 260 (4th Cir. 2011) (“[A]n adverse inference is properly drawn ‘against a party who fails to come forward with relevant evidence within its control.’” (quoting Norfolk & W. Ry. Co. v. Transp. Commc’ns, 17 F.3d 696, 702 (4th Cir. 1994))).

171. See, e.g., Bracey v. Grondin, 712 F.3d 1012, 1018 (7th Cir. 2013) (“In this circuit, when a party intentionally destroys evidence in bad faith, the judge may instruct the jury to infer the evidence contained incriminatory content.”); Hallmark Cards, Inc. v. Murley, 703 F.3d 456, 461 (8th Cir. 2013) (“[W]e conclude that a district court must issue explicit findings of bad faith and prejudice prior to delivering an adverse inference instruction.”); Dalcour v. City of Lakewood, 492 F. App’x 924, 937 (10th Cir. 2012) (requiring showing of bad faith for both permissive and mandatory adverse inference instructions); United States v. Nelson, 481 F. App’x 40, 42 (3d Cir. 2012) (noting that “where there is no showing that the evidence was destroyed in order to prevent it from being used by the adverse party, a spoliation instruction is improper”); Leon v. IDX Sys. Corp., 464 F.3d 951, 959 (9th Cir. 2006) (holding that “a finding of ‘willfulness, fault, or bad faith’ is required for dismissal” (quoting Anheuser-Busch, Inc. v. Natural Beverage Distribrs., 69 F.3d 337, 348 (9th Cir. 1995))); King v. Ill. Cent. R.R., 337 F.3d 550, 556 (5th Cir. 2003) (holding that because “[a]n adverse inference based on the destruction of potential evidence is predicated on the ‘bad conduct’ of the defendant,” it requires a showing of bad faith); Bashir v. Amtrak, 119 F.3d 929, 931 (11th Cir. 1997) (“[A]n adverse inference is drawn from a party’s failure to preserve evidence only when the absence of that evidence is predicated on bad faith.”).
you of this evidence.” Four circuits permit the inference to be imposed in cases of unintentional loss or negligent conduct.\textsuperscript{172}

The remaining circuits try to bridge the gap and have an intermediate approach that talks about knowledge or recklessness.\textsuperscript{173} They’ve tried to get in between.

The Civil Rules Committee obviously attempted to address the circuit split. As I said, the original proposal that was published and commented on said: to impose an adverse inference the spoliator had to have acted willfully or in bad faith.

After the public comment period, the proposal has been rewritten. As I said, I’m going to show it to you in a minute. But now the spoliator must have had the intent to deprive another party of the information for use in the litigation.

Now I ask you, is that really any different from willful? You still have intended to deprive the other side. I don’t think you can do that accidentally. So I think it is still a willfulness standard.

But let me give you a thought. In addition to punishment and deterrence, there is a third function of the adverse inference, and that is remedial; namely, to ensure that the innocent party is not prejudiced by the loss of that relevant information which was caused by the spoliating party.

Those three purposes—deterrence, punishment, and remedial—have been conflated in a lot of the case law. Courts have applied the same standard for imposing the adverse inference without separating out the purpose for which it is given.

But the culpability of the spoliator, when you think about it, is completely irrelevant from the remedial perspective because the only evidentiary concern there is whether and to what extent the innocent party has been prejudiced. If there’s no prejudice, there’s no evidentiary imbalance to remedy. So that’s the background.

Now, there are different forms of this inference that are important to note. They’ve been conflated, too. There’s a mandatory adverse inference, a rebuttable presumption, and a permissive instruction.

And it’s hard to divide the three, but I tried to do it once in the Pension Committee case so I’ll read it to you.\textsuperscript{174} In its most harsh form, a jury can

\textsuperscript{172} See, e.g., Grosdidier v. Broad. Bd. of Governors, 709 F.3d 19, 27 (D.C. Cir. 2013) (noting that “the spoliation inference was appropriate in light of the duty of preservation notwithstanding the fact that the destruction was negligent”), cert. denied sub nom., Grosdidier v. Isaacson, 134 S. Ct. 899 (2014); Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 108 (2d Cir. 2002) (finding “culpable state of mind” factor satisfied by a showing of negligence).

\textsuperscript{173} See, e.g., Stocker v. United States, 705 F.3d 225, 235 (6th Cir. 2013) (“The requisite ‘culpable state of mind’ may be established through a ‘showing that the evidence was destroyed knowingly, even if without intent to breach a duty to preserve it’ . . . .” (quoting Beaven v. U.S. Dep’t of Justice, 622 F.3d 540, 554 (6th Cir. 2010)); Gomez v. Stop & Shop Supermarket Co., 670 F.3d 395, 399 (1st Cir. 2012) (requiring “notice of a potential claim and of the relevance to that claim of the destroyed evidence”); Vulcan Materials Co. v. Massiah, 645 F.3d 249, 259 (4th Cir. 2011) (requiring “willful conduct”).
be instructed that certain facts are deemed admitted and must be accepted as true. That’s obviously the mandatory.

At the next level, a court may impose a presumption that is mandatory. But that’s only a presumption, and therefore, it’s rebuttable.

The least harsh instruction would permit, but not require, a jury to presume that the lost evidence is both relevant and favorable to the innocent party.

If the jury makes that presumption, then the spoliating party’s rebuttal evidence could be considered by the jury, which would then decide whether to draw an adverse inference against the spoliating party. So those are the three levels.

Now, the Second Circuit addressed the distinction between these various forms of adverse inference just a year ago in Mali v. Federal Insurance Co., a really important case. In Mali, plaintiffs brought suit against their insurance company seeking indemnification under a fire policy for the destruction of their barn. Although plaintiffs said they had no photographs of the second floor of the barn, one of plaintiffs’ witnesses said that she had seen such a photograph. The insurance company moved for an adverse inference instruction as a sanction for withholding the photographs. And the trial court instructed the jury as follows:

In this case, evidence has been received which the Defendant contends shows that a photograph exists or existed of the upstairs of what had been referred to as the barn house, but no such photograph has been produced. If you [the jury] find that the Defendant has proven by a preponderance of the evidence, (1), that this photograph exists or existed, (2), that the photograph was in the exclusive possession of the Plaintiffs, and, (3), that the non-production of the photograph has not been satisfactorily explained, then you may infer, though you are not required to do so, that if the photograph had been produced in court, it would have been unfavorable to the Plaintiffs.

Notice there’s nothing about state of mind. “You may give any such inference, whatever force or effect as you think is appropriate under all the facts and circumstances.” That is the charge that the Second Circuit affirmed.

Now, this is still called an adverse inference although it’s clearly not a sanction. It’s clearly remedial, and nobody cared about state of mind.

The court noted that the word “adverse inference instruction” can be used to describe two different sorts of instructions; those given as a sanction for

---

175. 720 F.3d 387 (2d Cir. 2013).
176. Id. at 389–90.
177. See app. VII.
178. Mali, 720 F.3d at 391.
179. Id.
misconduct, and those that simply explain to the jurors inferences they are free to draw in considering circumstantial evidence.\textsuperscript{180}

In \textit{Mali}, the trial judge simply explained to the jury that the finding of certain facts may, but need not, support a further finding that other facts are true.

The circuit explained that because “[t]he court did not direct the jury to accept any fact as true” or “draw any inference against the Plaintiffs,” but rather “left the jury in full control of all fact finding,” the court was not required to make the predicate factual findings usually required to impose a sanction.\textsuperscript{181}

\textit{Mali} recognizes the distinction between a permissive and a mandatory adverse inference instruction and the need for two separate standards.

Here is the new proposal that has just recently been circulated a week or two ago.\textsuperscript{182} Two subsections of proposed Rule 37(e) are relevant to the discussion of adverse inference jury instructions.

So the way this rule is divided, we have (e)(1), (e)(2), (e)(3), (e)(4). I will not pay any attention now to (e)(1) or (4), except to say (e)(1) is the curative measures pretty much in the published draft. And hopefully that would not involve adverse inference instructions. In fact, it includes actions like taking more discovery or cost shifting or reaching not reasonably accessible sources. That’s the idea of the curative measures.

Subsection (2), which I do want to talk about, provides for remedies to be imposed when an innocent party has been prejudiced by the loss of ESI regardless of the spoliator’s intent.\textsuperscript{183} So that’s really the one I’ve been talking about so far.

The permissible remedies to cure the prejudice, it says, exclude terminating sanctions and adverse inference instructions, but do include things like preclusion of evidence and the deeming of certain facts to be admitted.

The proposed rule specifically declines—this is actual language—“to cast the burden of proving that prejudice on either the innocent party or the spoliator.”\textsuperscript{184} It just doesn’t want to tell us. The Discovery Subcommittee report acknowledges that the new proposed rule, and I quote, “does not state which party bears the burden of proving prejudice.”\textsuperscript{185} Instead, the

\textsuperscript{180}. \textit{Id.} at 392–94.
\textsuperscript{181}. \textit{Id.} at 393.
\textsuperscript{182}. \textit{See} app. VII.
\textsuperscript{183}. \textit{See} app. VII.
\textsuperscript{184}. \textit{See} app. VII.
\textsuperscript{185}. The Discovery Subcommittee’s note to the proposal as applicable at the time of the Symposium reads:

\textit{Subdivision (e)(3) applies to jury instructions that permit or require the jury to presume or infer that lost information was unfavorable to the party that lost it. Thus, (e)(3) covers any instruction that directs or permits the jury to infer from the loss of information that the information was in fact unfavorable to the party that lost it. The subdivision does not apply to inferences that may be drawn from evidence introduced during a trial or jury instructions that do not involve such an inference. For example, it would not prohibit a court, in an appropriate case, from allowing the parties to present evidence and argument to the jury concerning the}
And then the court is supposed to draw on its experience in addressing this or similar issues and may ask one or another party or all parties for further information. The rule and advisory note also decline to specify burden of proof with respect to (e)(1) or (e)(3), but that’s not my issue here because the context of (e)(1) and (e)(3) probably mean that the moving party, which is the innocent party, likely bears the burden of proof on the threshold findings in those subsections. But in (2), the prejudice one, the proposal specifically declines to assign burden of proof.

Now, (e)(3) is the one that permits the sanction of termination or the striking of a defense, or the imposition of an adverse inference and says, “[b]ut only.” You’ll find the word “only.” But only upon a finding that the party acted with the intent to deprive another party of the information used in the litigation.

And then if that happens, the court may instruct the jury that it may or must draw an adverse inference. So it could be a mandatory inference or a permissive inference. The jury may or must find that the information was unfavorable to the party that caused this loss or destruction.

In other words, after a finding of intent to deprive, which is very similar to bad faith, a court can then impose either a mandatory or a permissive adverse inference instruction.

Now, the Discovery Subcommittee and the note reveal that despite the use of the word “only” in (e)(3), there still leaves room for a permissible jury instruction that relates to the loss of information; and, in fact, does not meet the intent to deprive standard.

If we go back to (e)(2) we find that the advisory note leaves it open. What it says, and this is a quote, is that “[t]he subdivision”—that is (e)(3)—“does not apply to inferences that may be drawn from evidence introduced during a trial or jury instructions that do not involve such an inference.” For example—this is the note telling us—

For example, it would not prohibit a court, in an appropriate case, from allowing the parties to present evidence and argument to the jury concerning the loss of information. Nor would it bar a court from instructing a jury that it may determine from evidence presented during the trial—as opposed to inferring from the loss of information alone—whether lost information was favorable or unfavorable.187

So again, it uses the word “unfavorable” “to positions in the litigation.”

---

186. Id.
187. Supra note 185.
“These measures would be available under subdivision (e)(2) if no greater than necessary to cure prejudice.”\textsuperscript{188} What type of instruction might meet the above description? I decided to write one. It sounds a lot like \textit{Mali}, but here it is:

If you find from all of the evidence admitted during the trial that a party has lost or destroyed information relevant to the litigation that should have been preserved, and the loss or destruction has not been adequately explained, you may, but need not, infer that the information would have been unfavorable to the party who lost or destroyed it.\textsuperscript{189}

It seems to me that the note would permit that instruction under (e)(2) even though (e)(3) says you can’t give an adverse inference unless there is a finding of intent to deprive.

The real distinction then between a jury instruction subject to (e)(2) as opposed to (e)(3) according to the note, I think, is who hears evidence about the circumstances of the loss or destruction and draws inferences about culpability.

If the judge makes those predicate findings, then intent to deprive is required. But if the jury hears evidence and makes its own findings and draws its own inferences, then no such intent must be established.

However, this proposal does not set out a standard with respect to when an instruction, permitted under (e)(2) rather than (e)(3), can be given. So given the absence of guidance on the use of an instruction regarding the loss of evidence as a remedial measure, there’s room for an evidentiary rule.

So I thought about a proposed evidentiary rule. And that’s the last part of the talk, you’ll be happy to know. There are two possible approaches here.

In formulating a more specific standard for the imposition of a permissive instruction, there are options. One option is to permit the jury to hear evidence from both sides whenever there is an allegation that relevant evidence was lost or destroyed.

But permitting the jury to hear accusations of spoliation in every case too easily would unduly burden the court’s resources, in my opinion, because it would lead to a trial within a trial. Moreover, juries may give undue weight to any evidence showing that potentially relevant information has been destroyed, regardless of the circumstances surrounding the instruction.

In light of that, those concerns that I have, the second option, I think a better option, is to devise a limited judicial gatekeeping role through predicate factual findings, while still leaving the inference-drawing function to the jury.

There’s little debate that before any inference instruction can be imposed, the moving party must show that the opposing party lost or destroyed relevant evidence within its control that it had a duty to preserve. But because the central concern of the remedial inference is to mitigate prejudice, the court must be satisfied as a threshold matter that there’s no other way to obtain the evidence to prove the point.

\textsuperscript{188} Supra note 185.
\textsuperscript{189} See app. VII.
And because the innocent party does not usually know the contents of the lost information, it may not be fair to require that the burden to demonstrate that prejudice be borne by the innocent party.

As an alternative, mental culpability—although irrelevant because the only evidentiary concern is remedying prejudice—could be useful as a proxy for the contents of the missing evidence, and, therefore, the likelihood of prejudice.

In fact, many courts have recognized a sliding scale between prejudice and mental culpability. In Residential Funding, a very well-known Second Circuit case, the court said, “Where a party destroys evidence in bad faith, that bad faith alone is sufficient circumstantial evidence from which a reasonable fact finder could conclude that the missing evidence was unfavorable to that party.” The court went on to note that even gross negligence is sufficient to presume prejudice under some circumstances. The issue then is burden of proof and burden-shifting. If the evidence was destroyed with malicious intent, then there’s every reason to presume that the evidence would have been unfavorable to the spoliating party, and therefore, helpful to the innocent party.

Similarly, in my view, when evidence is destroyed with gross negligence or recklessness, a presumption of prejudice is appropriate. Only when the evidence is lost through negligence or without fault, then it seems to me the moving party should affirmatively demonstrate prejudice by a preponderance of the evidence.

Now, the last way to deal with this would be to address the risk of unfairly influencing the jury, which can be accomplished by a balancing test that sounds a lot like Rule 403.

Specifically, proof of the loss of evidence should not be presented to a jury at all if the potential for unfair prejudice to the alleged spoliator substantially outweighs the benefit of a jury instruction to the innocent party. The court would be the gatekeeper and would be tasked with applying the balancing test.

The final question implicated in the respective role of judge and jury is whether the judge must instruct the jury with this inference once the predicate findings are made.

And again, the answer, in my opinion, is yes because a central purpose of an evidentiary rule is to provide guidance and consistency. Once the predicates are met, the construction should be mandatory.

The judge has discretion, of course, to apply and determine the balancing test, but if the rule only stated a judge may impose the adverse inference instruction even when the predicate requirements are found, then the optional nature of that would gut its effectiveness.

191. Id. at 109.
192. Id.
193. Fed. R. Evid. 403 (allowing exclusion of evidence if its probative value is substantially outweighed by the risks of unfair prejudice, confusion, and delay).
OK. So I finally present my rule, my one and only chance to write a rule. What I suggest is just for fun, by the way. I’m not really serious right now about this being rule language, but it’s an idea of how to guide things if we had an evidentiary rule.

It has four or five parts. That makes it look like a rule. Subpart (a) says “Prima Facie Showing.” It’s the usual. To make a prima facie showing, you have to show that the lost or destroyed or relevant evidence was within the party’s control and there was a duty to preserve it.195

“Prejudice. The nonmoving party”—and that’s the spoliator—“may rebut a prima facie showing by demonstrating by a preponderance of the evidence that the lost or destroyed evidence would not have been beneficial to the moving party”196 in some way. You can get it elsewhere or it’s not material. It’s not relevant or there’s another replacement for it so it’s no harm done.

“Burden Shifting. If the nonmoving party cannot demonstrate lack of prejudice, but can show that the evidence was lost or destroyed without fault or through ordinary negligence, then the burden shifts” back “to the moving party”—that is the innocent party—“to affirmatively demonstrate prejudice.”197

“Balancing Test. If the moving party”—which again, is the innocent party—“carries its burden, the circumstances of destruction and the likely contents of the missing evidence shall be decided by the jury pursuant to a permissive adverse inference instruction, unless the risk of unfair prejudice

194. Judge Scheindlin’s proposed evidentiary rule reads:
(a) Prima Facie Showing. To make a prima facie showing for a permissive adverse inference instruction, the moving party must demonstrate by a preponderance of the evidence that the opposing party: (1) lost or destroyed relevant evidence, (2) within that party’s control, (3) as to which there existed a duty to preserve at the time of the loss or destruction.
(b) Prejudice. The non-moving party may rebut a prima facie showing by demonstrating by a preponderance of the evidence that: (1) the lost or destroyed evidence would not have been beneficial to the moving party’s case, or (2) a satisfactory replacement to the lost or destroyed evidence is available.
(c) Burden Shifting. If the non-moving party cannot demonstrate lack of prejudice but can show that the evidence was lost or destroyed without fault or through ordinary negligence, then the burden shifts to the moving party to affirmatively demonstrate prejudice as defined in (b).
(d) Balancing Test. If the moving party carries its burden, the circumstances of destruction and the likely contents of the missing evidence shall be decided by the jury pursuant to a permissive adverse inference instruction, unless the risk of unfair prejudice to the non-moving party significantly outweighs the benefit of the instruction to the moving party.
(e) Definition. A permissive adverse inference jury instruction is one that implies no fault or wrongdoing by the alleged spoliator, but simply explains that the jury is free to draw any inference it decides is warranted regarding the circumstances of destruction and the likely contents of the evidence, and to accord that inference whatever weight it deems appropriate.

See app. VII.
195. See app. VII.
196. See app. VII.
197. See app. VII.
to the nonmoving party,"198 which is the spoliator, outweighs the benefit to
the moving party, which is the innocent party.

Finally, “Definition. A permissive adverse inference jury instruction is
one that implies no fault or wrongdoing by the alleged spoliator, but simply
explains that the jury is free to draw any inference it decides is warranted
regarding the circumstances of the destruction and the likely contents of the
evidence, and to accord that inference whatever weight it deems
appropriate.”199

Thank you.

PROFESSOR CAPRA: Fantastic job Judge Scheindlin. Thank you. We
have David Shonka here to provide some responsive remarks.

MR. SHONKA: Let me begin as John mentioned and my other
government colleagues, by noting that my views are my own. And the fact
is, I don’t speak for any carbon-based life form anywhere near Washington.
So there you have it.

Let me begin by just talking about the effects of adverse inferences on
cases and on parties. And that is, these things are really serious. They have
consequences for cases.

And I don’t care if it’s a mild instruction, a weak inference, or a strong
one, or a heavy one, or a mild one, or however you characterize it, the fact
is, at the end of the day, the minute the judge is up there talking about
presuming that some lost evidence was deliberately—or not even
deliberately, but some lost evidence were to hurt the party who lost it,
you’re going to have a real problem with the jury as a practical matter.

The consequence of this is that parties, even before litigation or at the
very first sign of any litigation, start to over-preserve, and they over-
preserve very seriously.

Over-preservation has consequences. It is burdensome on the parties
who do it. It is expensive. And yes, I know we all like to think that, “Gee
whiz, storage space is really cheap. You can get a terabyte at Best Buy for
a few bucks. And a terabyte is a lot of information.”

It’s inexpensive maybe in that sense. But maintaining it, storing it,
protecting it, reviewing it when necessary, trying to go through it every
time you have an inquiry and collect it and identify it, that all becomes
very, very, very expensive.

And the fact is, I can tell you that I know of federal agencies that have
been logging every email that has come into them for some time. And they
sit there today with terabytes of information. And every time some random
dog bite case comes through the door, they find themselves having to search
through terabytes of information for the one or two items that may or may
not apply.

This is expensive. It is time consuming. It slows down the business
process, too, because sometimes they have to go through those terabytes of

198. See app. VII.
199. See app. VII.
information to find things they actually need to do business. So that’s the effect.

The question then is: What purpose does it serve in the litigation? And in my own sort of casual way, I look at inferences as being something that ought to be based in logic and in the facts that have been proven.

And, for example, you look at footprints in the snow, you can infer that somebody walked through there. If you look very closely at them, you might be able to infer that some little girl walked through there. On the other hand, none of that will ever tell you that the little girl was wearing a blue dress. You can’t go there.

When you talk about adverse inferences, think about that which has been lost. And in my mind, it has three possibilities. One is that either it was helpful to the party who lost it, and they just didn’t know it. Two, is that it was harmful to the party who lost it. Or three, given the huge volume of electronic information that is out there, it was totally meaningless. It might have been relevant in some sense, but it would have been duplicative, redundant, useless, whatever. It never would have made the grade.

So now you have, out of three probably equal possibilities—because you know nothing about it—you have an adverse inference going against a party simply because they lost it.

When you look at remedial provisions for the purpose of deterrence and punishment and making the other party whole, the question is: Are you really doing that or are you, in fact, handicapping or putting a finger on the scale of the litigation in a way that perhaps is unwarranted or that you don’t know for sure that is warranted?

So the problem, in a sense, is that in trying to provide a remedy, we may actually be making things worse with adverse inferences.

Now that said, evidence does get lost. And I ought to be here proposing something affirmative, not just bashing the current practice.

And so let me suggest something, but it’s not in the form of any rule. In fact, I personally tend to think this is an area where the courts ought to play with it for a little longer, and we ought to have more development in the decisions.

But we might ask a couple of questions. One is: Does the person who lost the information, did they have knowledge, actually have knowledge of the contents of the materials that were lost?

And if they did, then I think you can do a presumption that they lost it for the wrong reason. So that’s OK. But you need to have some evidence that they knew what it was that they were losing.

But the problem is that you don’t have the lost information so how can you show knowledge?

And I would suggest the next issue is really one of—and I hate to resurrect the term “materiality” because that, in fact, was driven out of Rule 401(b), I believe, some years ago.

But the fact is, maybe there ought to be some showing that the evidence that has been lost, the material that has been lost, would have somehow had
an effect on the litigation. It would have been material to the litigation, which is actually Rule 401(b), when you think about it.\footnote{\textit{See} \textit{Fed. R. Evid.} 401(b) (requiring that for evidence to be admissible it must tend to prove “the fact is of consequence in determining the action”).}

But in terms of who has the burden in that context, let me suggest that maybe the burden ought to shift, depending on the context.

In some cases, for example—and I look at Judge Maas’s opinion in the terrorism case in the Southern District where the issue was: Is somebody financing terrorist activities?\footnote{\textit{In re} Terrorist Attacks on Sept. 11, 2001, 440 F. Supp. 2d 281 (S.D.N.Y. 2006).} And the documents that are lost are bank statements. There, the loss of material is so obvious that if the losing party has some rational explanation, the burden ought to be on them to do it.

On the other hand, if you have a case where material has been lost, but people have attempted to recover and have produced huge amounts of information and attempt to overcome that, then the burden should perhaps shift to the person who has received the information to do a basic gap analysis and to take a look at it to see if there is something that they actually need or if it’s something missing that handicaps their ability to prove the case. Is there enough here, is the question, in order to try my case to a conclusion.

The one final comment I could throw in is maybe a touch of ethics. And that is, lawyers have a duty as officers of the court to be truthful. And at some point, judges need to sit back and look critically at what bloviating counsel are saying at any given moment about how bad the world is and how harmful a lost email may be.

PROFESSOR CAPRA: Thank you, David. Response, Judge?

JUDGE SCHEINDLIN: The only response is, of course, that the innocent party does not always know what has been lost. That’s the basic response. I appreciated all of what you said, except we can’t evaluate what we don’t have.

That’s always been the conundrum. If something is really gone and is not duplicated somewhere else, not found somewhere else, we don’t know what it is. And so it’s very hard to prove prejudice in terms of remedial effect. That may have to fall under deterrence or punishment. I don’t know.

But all I was trying to do is straighten out who has the burden to show prejudice because that’s the biggest gap of all.

PROFESSOR CAPRA: It’s very useful to tease this out, even if it doesn’t come to a rule, to tease out where these burdens lie. It’s very useful. Judge Grimm.

JUDGE GRIMM: The only thing I would say, you have—if you’re away from the point where you have the sanction based upon the fact that it was an intent to deprive from which the logical connection, it must have been harmful, absolutely is logical.

If you’re in an earlier area, then the notion that the judge allows both sides to come up with evidence allows the agency to say, “We’ve got a
budget of $100 million a year. This would take—if we were to do all these other things, it would cost us half our budget. We did this, this, and this. We produced these other things.” And that allows the jury then to hear the context of it. And that’s the leveling area in there.

No one disagrees that there can be consequences on either side of how you come out on this, either in limiting access to information to people who don’t have access to it, or in expense and punishment to other sides. But it’s that area in between where the evidence about the loss is presented, and the jury gets to do it. We trust juries to do that all the time.

And if there’s a compelling story as to why it didn’t happen—I’ve had a case where an adverse inference instruction went out there. It was still a defense verdict.

PROFESSOR CAPRA: And especially if it’s a mild one. But I do understand the point, any adverse instruction is—

JUDGE GRIMM: It’s not something you celebrate.

PROFESSOR CAPRA: Right.

MR. SHECHTMAN: The rule you started with used the language “presume.” “May or must presume.” Your instructions wind up being inference instructions. Is the rule meant to be—

JUDGE SCHEINDLIN: No, they’re predicate presumptions before you make the inference. And you presume relevance. That’s what you presume. Then you go to what the result of that, but they may infer from that. So they have to do two presumptions before they do the inference. That’s all.

PROFESSOR CAPRA: Judge Diamond.

JUDGE DIAMOND: Judge Grimm is closer to this than I am because he’s on the Subcommittee, but the reason for the Civil Rules Committee’s apparent waffling is the genesis of this was that general counsels were screaming bloody murder, “We don’t know—with the common law developing the way it is, we don’t know what to preserve. We have our employees preserving their old Chuck Berry records. We just don’t know what to do. Please create some sort of a standard that includes culpability.”

We had willful and in bad faith. And they said, “No, it’s got to be willful and in bad faith.” We said, “Isn’t one the other?” And they said no. And so that’s why we had this recent amendment.

PROFESSOR CAPRA: Well, if one was the other, then stylists would tell you get rid of one anyway.

JUDGE DIAMOND: Right. And that was discussed.

MR. SHONKA: Just one final point on this. When the rules were first proposed way back, the language—the preambles and the purpose and all—this was described as bringing uniformity of the law to the circuits and discouraging over-preservation, among others.

But when you look at the latest comments that came out a couple weeks ago, the Committee said, “We’re giving up on over-preservation and come to think of it, uniformity among the courts is not all that important either right now.”
So having walked away from the very purpose of the original proposals, what do we accomplish by issuing any rule right now without at least thinking about—

JUDGE GRIMM: I’m not sure I’d agree with that characterization.

PROFESSOR CAPRA: That’s a good take; not of this Committee, just for the record.

JUDGE SUTTON: Can I just ask one quick question?

PROFESSOR CAPRA: Yes.

JUDGE SUTTON: Judge Scheindlin, I’m just curious. What I took from your talk and from your proposed modification was, if you take out of (e)(3) the “may” or “must,” you just make it the mandatory. So your point is to distinguish between permissive and mandatory. And what you’re struggling with is (e)(3) seems to have permissive and mandatory language with this intent trigger.

JUDGE SCHEINDLIN: Actually, no.

JUDGE SUTTON: And then (e)(2) still seems to allow the permissive. That’s what I took you to be—

JUDGE SCHEINDLIN: But respectfully, no. I don’t have a problem, and I’d hate to see you take out the permissive out of (e)(3). I’m a fan of being nonmandatory anyway. So even in an (e)(3) context, there could be a reason why it should be sent to the jury, you may. For example, there’s other information. There’s so much other information. There are other sources—you know, the usual arguments. So even though the person did destroy with intent, it doesn’t have much consequence. So I want to keep the permissive in (e)(3). That’s not my—

JUDGE SUTTON: With the trigger of intent.

JUDGE SCHEINDLIN: Yes. I have no problem with that. I have a slight problem that (e)(2) says—and (e)(3) says you can only do it here, but the note and advisory to (e)(2) says, “Well, OK, there are times you can do it in (e)(2),” then there’s very little guidance.

JUDGE SUTTON: Now I understand. You would solve that problem by getting rid of the “may,” but you want to keep the “may.” So I think what you will really want us to do is make it clear you can’t use (e)(2).

JUDGE SCHEINDLIN: No. I want an (e)(2) for the evidentiary purpose of curing prejudice. I just want more guidance in (e)(2) and suggested the guidance. That’s all. When to do—when to do it, who has the burdens. How should the judge be guided, because first the judge is told no, no adverse inference—

JUDGE SUTTON: It’s a civil rule. We’re not going to do evidence.

JUDGE SCHEINDLIN: Well, I came to speak at an evidence conference.

JUDGE GRIMM: Well, 502 was a civil rule on evidence.

PROFESSOR CAPRA: Thank you, Paul.
VII. *DAUBERT AND ELECTRONIC INFORMATION EXPERTS*

PROFESSOR CAPRA: We’re going to turn to an issue about experts now and electronic information experts in one particular area. Dan Gelb is going to guide us through this.

MR. GELB: I’m Dan Gelb, and I want to thank Professor Capra for reaching out and inviting me here—because it is a real honor—and for everybody for attending.

My topic is: Does *Daubert* apply to challenges to computer-assisted review of electronically stored information? I thought I’d start off with Practice Point Number 7 from the Sedona Search and Information Retrieval: “Parties should expect that their choice of search methodology will need to be explained, either formally or informally, in subsequent legal contexts, including in depositions, evidentiary proceedings and trials.”

What the evolution of electronically stored information has really created is an inextricable tie between the discovery phase of litigation and the trial phase.

So “computer-assisted review” is the generic term for the overarching subject matter of things like keyword search terms, de-duplication, and near-duplication of documents. For example, reducing redundant email threads is typically something that is a popular topic in a lot of cases, as well as the use of predictive coding software applications.

I’m certainly not going to go over the intricacies of Rule 702, but I am including it in here specifically because I’m going to talk a little bit about 702(a) in a moment; same thing with *Daubert*.

What I think is important to keep in mind is that computer-assisted review tools are powerful and sculpt the direction of evidence in a case. So the subject has far-reaching implications on other evidentiary rules including best evidence, use of duplicates, and summary evidence. The review applied could potentially impact findings later on down the road on dispositive motion practice as well.

What we’re dealing with in a lot of ways is a situation where litigants are being placed between the rocks and the whirlpool when the review process of electronically stored information could adversely impact the evidence ultimately presented at trial, but there is no basis to challenge the methodology used because it may be viewed as a discovery rather than an evidentiary issue.

Now, when you think about predictive coding, and the main concepts of coding a seed set of documents, the goal is to train the computer to determine relevancy, by using technologies such as predictive coding.

---

203. For Mr. Gelb’s PowerPoint presentation, see Appendix VIII.
204. See app. VIII.
205. See *Fed. R. Evid.* 702 (requiring, among other things, that an expert’s testimony must be based on sufficient facts or data, and must be the product of reliable principles and methods reliably applied).
modules in software applications to search that seed set and reinforce the process with quality control.

What I think is interesting about the concept behind what the predictive coding factors are is, in a lot of ways, similar to certain things about the gatekeeping factors under Daubert.

I think that’s a real interesting tie in that regard because the Daubert review has traditionally been applied to trial testimony, but you’re now dealing with determining evidentiary issues extremely early on in cases which can sculpt the direction of the evidence at a later point in time.

Some courts have begun to review predictive coding. In the interest of time, I’m not going to go through the specifics case by case, but what I think is really interesting is this first case out of the Delaware Court of Chancery. There was a sua sponte order, which appears from what I read from the case to use a predictive coding process in that matter.

There’s the well-known Da Silva Moore case. It’s created a lot of conversation.

Kleen Products, a Sherman Act class action. What’s interesting about Kleen Products, I think, is that it cites to United States v. International Business Machines and observes that discovery is most broadly allowed in antitrust litigation because conspiracy is a difficult thing to establish. And it goes into an in-depth discussion of technology-assisted review.

As well as In re Actos, in which the court goes into real, real nitty-gritty on predictive coding and how the statistical analysis disciplines are used in that context.

Now, the first question I’m thinking about is: Can Daubert apply to computer-assisted review in the first instance? One problem is that Rule 702(a) purports to regulate experts who will “help the trier of fact.”

Now, Rule 702(a) is, I think, something that a lot of the cases seem to be really predicated on because you have the issue of whether one can even apply Daubert in the first place as a matter of jurisprudence.

But if the issue is that the application of Daubert is not procedurally ripe unless the fact-finder is presented with an evidentiary question, then the real conundrum is: What is the procedural tool that can be asserted if Daubert and Rule 702 are relegated to the fact-finding process, and not to the...

---

211. Fed. R. Evid. 702(a) (“A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if: (a) the expert’s scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue . . . .”).
reliability of discovery methods—especially ones as complicated and technical as predictive coding?

It’s a real catch-22, and that’s what I mean by placing litigants between the rocks of a discovery dispute concerning computer-assisted review and the whirlpool of the same disputed issue at trial, which is a very important distinction to think about.

Now, the type and volume of ESI differ across litigations—both civil and criminal—including complex cases, class actions, even cases that may have not as many documents involved. There could be, however, complex forensic components to it that call for technology-assisted review.

Note an interesting interrelationship under Rule 26(f) and the Advisory Committee Notes for the Federal Rules of Civil Procedure: “In appropriate cases identification of, and early discovery from, individuals with special knowledge of a party’s computer systems may be helpful.”

So I think as a general proposition, the system seemed to be trending toward the idea that we need to have a heightened level of knowledge when it comes to how electronically stored information impacts cases on a macro level.

Once again, should Daubert apply to computer-assisted review? Is the technology-assisted review product being used verified and tested? Computer-assisted review is inherently based on science and is derived from other things like statistical analysis.

Another important distinction is that modules with computer system review are a la carte a lot of times, and are not necessarily a price-fixed menu. There are different components to the software. There are different characteristics to the different types of proprietary software that various different e-discovery service providers offer.

So it’s important to think about how these products work behind-the-firewall because the methodology could have far-reaching impacts depending on the type of evidence that you’re dealing with, if there isn’t an in-depth, expert-based analysis being conducted on the actual process.

Now, what I’m going to close with is a theoretical paradox, which is, in theory: the same court that allows a particular approach to computer-assisted review could later find the evidentiary results fail under Daubert at trial. Therefore, it makes good sense to apply the gatekeeping process of Daubert at an earlier phase, even though the trier of fact is not involved.

PROFESSOR CAPRA: I did a predictive coding case as a special master. And lawyers can’t talk to you without talking to the IT people first.

I couldn’t see how I could figure out the dispute between the parties about how the predictive coding would work without having some IT person explain it to me. Maybe courts are being hypertechnical about saying Daubert doesn’t apply here because it’s pretrial. Maybe Daubert is not the issue, but is there some kind of scrutiny that needs to be required to see that the plan is defensible?

---

JUDGE GRIMM: *Daubert* is entirely based upon the notion that—it’s the old adage of garbage in, garbage out. If your facts are not sufficient and your methodology is not reliable, then it’s not relevant because it has no tendency to prove anything.

And as far as I can see, it’s a false debate because the question is: in the pretrial process, if you want to convince the court that you have done what you have to do to produce this evidence—because you’re saying it is cheaper to use this process—then the question is whether it’s a reliable process that is based upon scientific principles that are reliable. It manifestly is scientific, technical, or specialized.

So you’re right smack into what Rule 702 talks about, and the judge doesn’t have the ability to rule on the discovery plan without the assistance of reliable experts. Why would you ever want to say the tools that help you get reliability cannot be used to try and help the judge make that decision?

PROFESSOR CAPRA: The judge is in the same situation as the trier of fact would be if there were no *Daubert* inquiry.

JUDGE GRIMM: Are you trying to decide this is reliable methodology so that you can use the result in either a pretrial or a trial context? Perhaps the conceptual problem is that *Daubert* has acquired a secondary meaning of this very expensive, four-day hearings, experts that you can’t figure out what they’re saying, bring them in and bet the ranch on the costs.

You don’t have to do it that way. The judge has the tools to be able to do it in a way which is much more streamlined. That’s just effective case management. But to say that you can’t use tools that are designed to help you get reliable information, and whether the output can be relied upon, strikes me as being self-limiting for no reason.

PROFESSOR MARCUS: I’m the guy who wrote that note on Rule 26 that was referred to in Dan Gelb’s presentation. Ten years ago, there was no such thing as discussion of predictive coding. We were talking about Rule 30(b)(6) type things or just bringing your experts to the conference.

I think with regard to what Paul Grimm says, if they’re using this to produce evidence they’re going to put before the jury to prove there’s nothing in our records that says X, then that’s a Rule 702–type problem.

But I think the guidance Rule 702 might provide in doing the case management might be useful without the full dress hearing. I don’t think you’re saying that once discovery has been done and this email has been found, the admissibility of the email has anything to do with Rule 702.

So it’s really not an evidence rules problem. It’s just about how are we going to find—what are we going to look for and how hard are we going to look.

MR. GELB: But respectfully, wouldn’t the process employed at the beginning of a case impact the relevance of a particular resulting document that may or may not have been discovered in a particular context because of

213. *Id.*
the technology applied in the beginning? It could impact the trial evidence later on down the road, such as pattern of conduct.

PROFESSOR CAPRA: And I guess the point is, even if it doesn’t, you have to have a defensible plan; and that’s something for the judge to decide. So it’s the at-trial and it’s the pretrial.

I think we have it figured out that it should be a Daubert-type analysis of the computer-assisted discovery plan, even if you don’t call it a Daubert analysis. Thanks, Dan.

VIII. RULE 502, THE GRAND JURY, AND PRIVILEGE

PROFESSOR CAPRA: We’re going to move now quickly to privileges, and specifically, Rule 502.214 We had a whole seminar about Rule 502,215 but there is a question about its applicability that we did not discuss at the prior symposium, as well as an issue about Rule 502 and the extent of its protection in criminal cases, especially regarding electronically stored information.

MR. GOLDSMITH: Thanks, Professor.

In contrast to many of the other speakers, as opposed to being here advocating a new rule, what I’m really seeking—and Dan and I talked about this a year ago—is what can be best described as post hoc Advisory Committee Notes or gloss to make it clear that Rule 502(d) is intended in criminal cases to apply in the grand jury context.216

The typical fact pattern is actually not only simple, but I’ll say this much from the perspective I have in this position, which is national in nature for the last four-and-a-half years—it is the recurring issue in federal criminal cases.

If there’s a question, and I know this comes up at conferences regularly: What has been the effect of 502(d)? How often are we seeing it applied? Probably the main reason it’s not being applied in federal criminal cases is because of uncertainty on the part of prosecutors and arguably even more importantly, criminal defense attorneys, as to whether it applies where it really matters—in the grand jury context.

And the fact pattern, as I said, is very simple. A witness receives a grand jury subpoena. It calls for ESI. The ESI may be cloaked with attorney-client privilege, some of it at least, or work product protection.

The recipient states, as happens in civil litigation all the time, this could take months to go through with a fine-tooth comb. I’m willing to do an expedited review, but I have concerns about potentially waiving privilege.

214. FED. R. EVID. 502 (providing for certain protections against waiver of attorney-client protection and work product).
216. Rule 502(d) provides that a federal court may order that the protection of the attorney-client privilege or work product doctrine is not waived by disclosure in connection with “the litigation pending before the court—in which event the disclosure is also not a waiver in any other federal or state proceeding.” FED. R. EVID. 502(d).
Whether raised by the grand jury subpoena recipient or by a savvy prosecutor, how about a clawback agreement? The discussion goes, well, that will work as between us, the United States, at least in the criminal case, and the recipient, but what about third-party litigation, in particular shareholder suits or anything else down the road?

And assuming that the entities have sufficient sophistication, they go, “Ah-ha, what about Rule 502(d) orders?” The potential undoing of the ah-ha moment is the requirement in Rule 502(d) that the disclosure occurs “connected with the litigation pending before the court.”\textsuperscript{217} At best, it’s ambiguous, and, at worst, it’s not litigation pending before the court when you simply have a grand jury matter in effect.

So the question then becomes: What procedural step needs to take place in order to obtain that Rule 502(d) order so that it would be effective going forward?

The procedural step one could argue could come from either the prosecutor filing a motion to compel or the recipient filing a motion to quash. And then the case gets assigned quite naturally to the grand jury judge. And whether it’s, you know, logged as a miscellaneous matter or not, I’m not really sure that’s all that critical.

The components of the Rule 502(d) order would very much track the model order that came out of the symposium in October 2012.\textsuperscript{218} You’d have a truncated privilege review. You’d have no waiver by disclosure. You’d have notification requirements. You’d have best efforts.

The burden of proving privilege would be on the person claiming the privilege. And the piece that would be clearly unique to criminal cases—and it’s one that several people in the room have given me some input on, as well as you can imagine, quite a number of prosecutors around the country—is this whole \textit{Kastigar}\textsuperscript{219} issue lurking below the surface. That is, whether the privilege protection extends to the fruits of the privileged information that is disclosed pursuant to the Rule 502(d) order.

There was actually some pretty clear law in the \textit{Warshak}\textsuperscript{220} opinion, which seems to be the one-stop shopping for seemingly everything in the ESI realm. But in \textit{Warshak}, the Sixth Circuit noted that in its view, \textit{Kastigar} is inapplicable to violations of evidentiary privileges and cited the Fourth Circuit \textit{Squillacote}\textsuperscript{221} opinion.\textsuperscript{222} Meaning that fruits would not be protected.

As Dan and prosecutors in the Second Circuit have pointed out, you have the \textit{Schwimmer}\textsuperscript{223} case, which at least goes through the analysis, concluding

\begin{flushright}
\textsuperscript{217} Id. (“A federal court may order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court—in which event the disclosure is also not a waiver in any other federal or state proceeding.”).
\textsuperscript{219} \textit{Kastigar} v. United States, 406 U.S. 441 (1972).
\textsuperscript{220} \textit{United States v. Warshak}, 631 F.3d 266 (6th Cir. 2010).
\textsuperscript{221} \textit{United States v. Squillacote}, 221 F.3d 542 (4th Cir. 2000).
\textsuperscript{222} \textit{Warshak}, 631 F.3d at 293–95.
\textsuperscript{223} \textit{United States v. Schwimmer}, 892 F.2d 237 (2d Cir. 1989).
\end{flushright}
that fruits are in fact protected, although finding that there was no privilege waiver there.\textsuperscript{224}

Any 502(d) order in this context, rather than roll the dice as to what the courts would do, clearly would have express language not unlike your standard proffer agreement where if the government has already reviewed the information, subsequent to a subsequent claim of privilege, there’s no limitation placed on the government’s use of the information, evidence or leads derived directly or indirectly from the information subject to the claim.

Without that, I will tell you I can’t imagine any prosecutor would be willing to receive documents, have the recipient and say, “Oops, I’ve discovered something.” And then down the road run the risk that the entire investigation, as well as the prosecutor’s own participation, could have been tainted as fruits of the privilege information.

I will say this much: having discussed this with not only some of the judges in this room, but practitioners around the country, they want to have this protection of a Rule 502(d) order during the grand jury phase. When I say “practitioners,” I mean criminal defense attorneys.

But they want a high enough comfort level, whether it’s for their clients or perhaps between them and their clients, that they’re not going to have been found to have done something that puts the client in harm’s way down the road, that is, a subsequent finding of waiver by disclosure.

I do think that the kind of discussion that hopefully will follow my teeing up this issue, which will be reported in the \textit{Fordham Law Review}, as well as, maybe a short law review article making this point, it’s not going to be the same thing as the rule itself saying it—

PROFESSOR CAPRA: Who has to write that article?

MR. GOLDSMITH: Well, that—to be discussed. I can imagine who the likely person who would draw that straw would be.

But it’s not going to be the same thing as if the rule expressly said it. It probably won’t be as good as if there were Advisory Committee Notes contemporaneously. But if there is (1) as will be clearly the case, minutes in the \textit{Fordham Law Review}; (2) maybe a short article; and (3) a test case where a district court judge said, I am ruling that this—that Rule 502(d) applies among other reasons because I think the clear language, as well as the discussion cited in the \textit{Fordham Law Review}, supports that notion, I do think that could go a long way to function almost as a seed crystal going forward and giving practitioners around the country, as well as prosecutors, a higher degree of comfort.

And then I think you could see the explosion of application of Rule 502(d) orders in criminal cases as was hoped for.

PROFESSOR CAPRA: I’d like to turn it over to Judge Diamond, who was our commenter on criminal cases at the Rule 502 symposium, for his reactions.

\textsuperscript{224} \textit{Id.} at 243–45.
JUDGE DIAMOND: The idea that there’s a safety net so that if privileged documents are unwittingly or unintentionally turned over to the grand jury, that the privilege isn’t waived, I think is a good one.

But that’s not really what you’re proposing here. The materials you sent around last night say, “to help expedite the process,” meaning the production of documents in response to a grand jury subpoena *duces tecum* while keeping down the costs of privilege review.

They talk about a truncated privilege review. A truncated review of the documents, you give them over, and then you say to the government, if you find anything that’s privileged, you give them back.

I would ask Paul Shechtman if he were representing a corporation that’s being criminally investigated, and you get a grand jury subpoena for documents whether or not it’s going to be over your dead body the documents go out without you looking over each and every document, if there’s possible criminal ramifications.

Otherwise, Paul would be saying to the president of the company, “The bad news is, the email I sent you explaining in great detail how you broke the law in five different ways has been given over to the government.”

The good news is, they’re going to give the document back. The bad news is, they can investigate the heck out of you based on the information you provided.

MR. SHECHTMAN: And the good news is, or the bad news, also, it’s easily authenticated.

JUDGE DIAMOND: Very easily authenticated, by the fact of your producing it. I just can’t imagine competent counsel doing that. As I say, as a safety net, if we unwittingly, unintentionally we go through everything and something still gets through, please give it back to us, sure.

PROFESSOR CAPRA: That’s actually protected under 502(b), which does apply to your situation; right? Because it’s a proceeding; grand jury proceeding is a proceeding like any other.225

JUDGE DIAMOND: It is. But if it’s your company or your person, it’s a privately held corporation, and you own the company, and it’s you who is on the line, the Rule 502(d) order would be scant comfort to me.

MR. GOLDSMITH: If I may clarify. I’m not suggesting, Judge Diamond, that the answer to your receiving the grand jury subpoena does a four-day slapdash job. What I’m talking about is the difference between, as I interpreted the order coming out of the *Symposium on Rule 502*,226 doing a reasonably thorough, but less costly—I’ll make this length up—a two- or three-week review as opposed to eighteen-month review, which is what you might hear from the entity in question.

225. Rule 502(b) provides that even in the absence of a court order, a disclosure of protected information to a federal office or agency is not a waiver if the party took reasonable steps to prevent disclosure and promptly sought return of the material after the disclosure was discovered. FED. R. EVID. 502(b).

226. See supra note 218.
JUDGE DIAMOND: Again, having done criminal work before I landed on this august perch, I would not allow a document out, any document out, unless a mature, sane, responsible adult representing the entity subpoenaed had read over the document first in a criminal investigation as opposed to civil discovery. It’s just very, very different.

PROFESSOR CAPRA: Maybe that’s why Rule 502(d) is not being used in criminal cases.

JUDGE DIAMOND: And that’s why I checked with the head of the appeals unit in our U.S. Attorney’s Office. He said there’s use of clawback agreements. The defense attorneys wouldn’t be that stupid to give us this stuff and say, “Oh, here, you can have it back, but let’s investigate what we learned.”

PROFESSOR CAPRA: I can state that this particular issue that Andrew raises didn’t get brought up during the process of drafting Rule 502, that is, the applicability of Rule 502(d) to grand jury proceedings. I think the idea was that there would have to be a proceeding in front of a judge. That was always the idea.

JUDGE GRIMM: Otherwise, the judge can just issue an order without a case before them saying this is off the record. And it’s civil, and it’s all cases, federal and state. That was the worry about that.

PROFESSOR CAPRA: I guess it wasn’t discussed. I don’t know what kind of comfort we can give in this situation.

John, did you have a question?

MR. HARIED: I accept what Judge Diamond said with regard to the company that’s the target of the grand jury investigation. Would it be different with regard to a company that’s just a third-party records custodian?

JUDGE DIAMOND: Oh, I expect so. I expect so.

MR. GOLDSMITH: Maybe I should have clarified that in the point. That’s not every entity obviously that receives a grand jury subpoena.

JUDGE DIAMOND: Even then—even then, if I were representing the company, I would say as responsible counsel, you’re not the subject. You’re not the target. Some prosecutors are very, very good about being candid and honest about—no one is dishonest—about being realistic about who is a target and who is not.

Other prosecutors write the word “target” on your forehead while they’re putting the handcuffs on you, and—

PROFESSOR CAPRA: You never know.

JUDGE DIAMOND: You just don’t know. And so if you’re acting responsibly, you tell your client, I’m sorry it’s going to cost you so much money, but you don’t want to give over these documents unless the lawyer representing you has gone through each and every one.

If, in fact, it’s perfectly clear to everyone you’re simply a witness, simply a third-party witness, maybe. Maybe.

MR. GOLDSMITH: I will tell you from the experience and the feedback that I’ve received, more often than not, you hear that the idea is initiated by
the entity that receives the grand jury subpoena where their attorney doesn’t want to have their client bankrupt by what would be full, thorough review of the sort that you would put if you had company litigation involved.

And if the view of the group at large here is that it’s too risky no matter whether you’re a target or just a mere recipient, I don’t want to carry the brief for defense attorneys around the country. That’s not my job.

JUDGE GRIMM: For the entity that doesn’t worry that it’s going to be a target, or it just wants to get the information out without having to spend all the time and money to do so, and also is worried about the possibility that if it’s a consumer product investigation on some sort of regulatory crime, that they’re going to be opening up the door to massive class action litigation, then a Rule 502(d) order would be very useful in that context.

And a vehicle can be found for doing it, whether it’s a motion to quash or a motion for protective order or a motion to compel, that then puts a proceeding before the judge who can then use Rule 502(d), and the protection falls in place.

PROFESSOR CAPRA: Create a proceeding.
JUDGE DIAMOND: That’s simple enough.

IX. THE SHOPBOOK RULE AND THE ROLE OF EVOLVING TECHNOLOGIES

PROFESSOR CAPRA: And now we have our futurists. And so we start with George Paul. And then Paul Lippe.

MR. PAUL: I’m not going to try to predict the future because everybody knows that’s impossible, but I want to suggest that you can see into the future a little bit. You can have a vision of the future.

And technologists very much believe that you can do that, if you know what the hard trends are in society and if you understand the relevant laws that are in operation.

So I think the first step is: you look very closely at what’s right in front of your face. What are the undisputed facts about what we’re confronted with right now?

Have you noticed that recently, everybody has started looking at these little devices called smartphones? They’re getting more and more advanced each year. This is a big deal to technologists. It relates to what is called “technique.”

Technique is a French term that refers to the way society is interacting with and using its technology. So this societal addiction to these ever-increasingly advanced mobile devices is a profound development.

They enable transactions galore. You know what I’m talking about. There are now more mobile devices than there are people on earth. This is a worldwide phenomenon that is new to the planet earth.

Next thing. Everybody has heard about the cloud, the cloud, the cloud. What is all this rigmarole about the cloud? Well, the cloud is extremely important. It is a revolution in business models that dramatically lowers the cost of production, the costs of computation, and the cost of storage of information.
And now the computer systems. Now, they’re all over the world. They’re virtual. “Where is my data?” “Oh, I don’t know, it just moved over to Singapore last week. We don’t know where it is.”

With the virtualization of the economy, there are dramatically lower costs. Huge databases can be accessed in real time by supercomputers. This is not something that only IBM can do. No. Everybody gets to do it right here on their cell phone. It’s called an “app.”

You’re accessing huge databases in the cloud instantaneously. Just think of what you can do: Where is the nearest this or that? Your phone knows exactly where you are. It has a database of all the goods and services. It can read bar codes. They even have apps that tell you how you can control your mind. How many apps are there? There are now over one million apps. That’s a lot of apps.

Another new development has occurred. New networks of minds are springing up. I’m talking about “mind networks.” We kind of pooh-pooh it. Oh, it’s just social media. But it’s profound.

You know, in social media, you can go from one person’s mind to 100 million people’s minds in six days. So far, that’s the fastest viral growth of a message. That’s a revolution in publication technology.

By now this is all obvious. We sort of take it for granted now. But if you start really observing, what’s a little further out on the horizon is something called intelligence in objects, intelligence in things.

Things are becoming increasingly intelligent. They have these intelligent basketballs with little chips in them that will send out signals to a database. How are you dribbling? How are you shooting?

They have intelligent tennis rackets. They have intelligent bridges and intelligent roads. They have intelligent refrigerators. They’ve got intelligent dirt. They put chips in cows and cows are now intelligent.

What is well-accepted in the industry is that these objects are going to become increasingly intelligent in the future. And how is this? Why is this? It is because one of the aspects of computer technology is a mind-blowing miniaturization of chips and of devices.

So what they’re going to be able to do, and what they’re doing now is, they are putting electronic devices on things. You know how big such devices are? They’re small enough to be glued to the back of an ant so that scientists can study the ant’s behavior.

And they’re sending out signals wirelessly. Did you know that the smallest device that’s manufactured is as big as a speck of dust? And they have cameras that are one cubic millimeter. So there’s a mind-blowing miniaturization going on.

Now, what if you took all these things with all these miniature devices on them, and you hooked them up to an internet on steroids? That sounds pretty interesting. Well, guess what? There is an internet on steroids that’s being constructed right now.
People are devising a new internet protocol called IP Version 6.\footnote{For more information, see generally FCC CONSUMER TASK FORCE, INTERNET PROTOCOL VERSION 6 (IPV6) CONSUMER GUIDE (2014), available at http://transition.fcc.gov/cgb/consumerfacts/ipv6.pdf.} It’s already rolling out. It allows more IP addresses than there are atoms on the face of the earth.

You might think, “That sounds incorrect. Oh, he must be making a mistake. That’s fantastic.” I say, just go look it up. It’s true. The infrastructure for a mind-blowing internet is right in front of our face. We’re talking three, four, five years, maybe eight years out.

When you have networks, you have incredibly powerful dynamics. When you have networks, you have something that’s called “complexity.” Recently they discovered people were using a refrigerator to send out spam. So you see the emergence of a new kind of animal.

The next thing I want to talk about is that everybody in this room has a cognitive disconnect. And that’s because of the concept of exponential growth.

Your mind does not comprehend exponential growth. Let me just give a very brief kind of mind experiment. Bear with me for just a moment as I explain something to you.

If I have a chessboard here, and I say, “Here’s a penny on the first square. Here’s two pennies on the next square. Here’s four pennies on the next square. Let’s double them once a minute for about an hour.” Just think. Use your intuition. Use your societal intuition, your personal intuition. How much money would you have on that last square after about an hour? Don’t blurt it out. Just honestly, sincerely use your intuition. How much money would you have? You know it’s big.

The answer: you’d have one thousand times the global gross domestic product on that last square.

Now, were you off by a factor of a million? Were you off by a factor of a billion? I don’t think if you’re a public policymaker it’s prudent to be off about a relevant process by a factor of one billion.

Now, why am I talking about this? Because it’s known and well-settled that computer technology grows in precisely the same fashion and with the same sort of acceleration.

Let me just show you this little device. I think you can get it for $9.99. It’s a thumb drive, sixteen gigabytes of memory. How much did this cost when the Federal Rules of Evidence were adopted? Four million dollars.

How big was this thing when the Federal Rules of Evidence were adopted—this storage of sixteen gigabytes of memory? The storage required the size of a room this big with a bunch of refrigerator-sized machines in it.

Now, that ought to tell you something. We take this for granted now. If I lost it, $9.99, it’s no big deal. No. We’re talking about something that has changed so dramatically since these rules were enacted that we go from a giant multi-ton thing costing $4 million to a little toy.
The cognitive disconnect is critical. How much more powerful will computer technology be when our kids are our age? How much? You know it. You’re the public policymakers. You’ve studied this very carefully, I’m sure. Computer technology will be one million times as powerful as it is today.

What happens is that you’re accelerating and growing higher and higher. And you double and double and double. You start racing toward the sky with your processes. And that’s what we’re doing now.

So I think in the context of where are we now, what are we doing, I think you have to realize and say to yourself, “I’ve got a cognitive disconnect. Something’s going on. Something important is happening. I know it. I can sense it. This is what has happened.”

So why am I talking about this? Well, before I go to the past, I started off with the future. I’m going to go to the past now—to the Rules of Evidence. What the technologists say—very respected ones—and this is what you need to put it in perspective: what is occurring and what will occur over maybe the next ten, twenty, thirty years is the biggest development in civilization since the invention of the printing press.

The printing press ushered in modernity. But what we see now we take for granted. We’re living now and our attitude is: “Of course, this is not the biggest thing since modernity.” No, you are indeed living right now during an event that is the biggest development to emerge since modernity. And again, as public policymakers—people who are designing the Rules of Evidence—that’s something to keep in mind.

What has happened is that there has been the rise of something called the “complex information system.” I see the use of the term “machines” in some of the literature. But these aren’t machines. These are information flows. They’re mind-bendingly complex.

Thousands and thousands of people are writing software. There are tens of thousands of server operators and people misusing systems. Now people are shooting information into other people’s minds in immersive experiences.

The jury research shows that the consumption of immersive digital information can change one’s memory and even implant false memories and so on. So there’s a new kind of declarant that has arisen in the law. It is called “complexity.” How do we comprehend it?

And this is where the law gets very confusing.

There’s a huge jurisprudence on the topic of the statements of machine systems. I heard it discussed this morning. “Oh, if a machine says it, it’s not a statement.” No. It’s not a declarant. It is therefore not covered by the hearsay rule.
And the Confrontation Clause jurisprudence that was in Professor Capra’s excellent memo\textsuperscript{228} says the same thing. Oh, if a machine says it, we don’t have to worry about it. It’s not a statement. It’s not a declarant.

And if one looks at Rule 803(6),\textsuperscript{229} it talks about “someone” doing something. It’s a “someone.” Why does it say “someone?” Well, because if you really study the law of evidence, that rule, 803(6), is four hundred years old.

It’s kind of hard to believe really. In the late 1500s in preindustrial times, the shopkeepers started writing transactions down. And the judges started receiving their “shopbooks” into evidence.

Well, Parliament noticed this. And it said, “We don’t know if we like this. The shopkeepers aren’t ‘crossing out sums.’ They’re not ‘crossing things out.’”\textsuperscript{230} And oh, by the way, Parliament’s attitude was that such records are also self-serving, but the upshot: we have to use them nevertheless.

So what parliament did in 1609 was pass an act that said, in effect: “Well, you can use them, but only for a year.” So that was the rule of evidence in our courts as early as 100 years before the law of evidence emerged in the early 1700s.\textsuperscript{231}

The American colonies adopted this rule. It was used right through the middle of the 1800s because, before the Civil War, all business records were in handwriting. So the shopbook rule was still working and enforced.

After the Civil War, the people that made the guns, Remington, started manufacturing typewriters. And the typewriter diffused throughout the economy. And we had typewriters, and we had carbon paper. The shopbook rule still worked fine.

Now, the biggest information technology development in between the typewriter and the computer was the vertical file cabinet. It was a revolutionary technology, allowing you to organize your business documents with much greater efficiency.

And in the 1920s and 1930s, vertical file cabinets spread throughout the country. They were made of wood at the time. Steel vertical file cabinets didn’t come into the fore until after World War II.

But in the early 1900s, there was—and I still see it today in this room—a call to a codification of the law of evidence. There was a famous speech made in 1906 by Roscoe Pound urging the modernization of the law of


\textsuperscript{229} FED. R. EVID. 803(6) (providing a hearsay exception for business records).

\textsuperscript{230} See Paul, Systems of Evidence, supra note 5, at 186 (discussing Radtke v. Taylor, 210 P. 863 (Or. 1922)).

\textsuperscript{231} For background, see Radtke, 210 P. 863, as discussed in Paul, Systems of Evidence, supra note 5, at 185–87.
evidence, and its codification.\textsuperscript{232} Everybody started trying to codify, codify, codify.

As a result the shopbook rule was codified in 1927 as “The Commonwealth Fund Act.” Just read the Advisory Committee’s Note to Rule 803(6). It indicates that the rule was modeled almost directly after the Commonwealth Fund Act of 1927. Congress largely, if not verbatim, adopted the language of that Act in 1936.\textsuperscript{233} That was the evidentiary rule of the federal courts as of that year and it has not changed since that time.

Accordingly in the 1930s, by statute in the federal courts, we had a codification of a rule that arose in the late 1500s. There was no need to change it. Business processes and records were largely the same as before. The shopbook rule then became recodified as Rule 803(6) in the 1970s, and that rule was taken from the 1936 federal statute, which in turn had been modeled after the 1927 Act. The rule now still talks about a “someone”—not a complex information system.

These complex information systems sense things. They decide things. They record data. They have complex algorithms which transform information. They’re not just recording things.

So I would, in conclusion, suggest that you really think about the cognitive disconnect. You think about the new declarant in the law. You think about the fact that the hearsay rule is adrift. For the most important information that is being created in society, there is no rule of evidence that exists today that can be used to gauge and test its reliability.

All this is particularly important because the law of evidence—as expressed in the Federal Rules of Evidence—not only controls the admission of evidence in our courts, it represents how society differentiates true from false and thus right from wrong. Unless the law of evidence evolves with society, the rule of law may be in jeopardy.

PROFESSOR CAPRA: Thanks, George.

MR. PAUL: You’re welcome.

PROFESSOR CAPRA: So we close with our other future thinker, Paul Lippe, who I want to thank for being patient and coming all the way up here for this talk. Both our future thinkers made a lot of sacrifices to get here. I appreciate that.

MR. LIPPE: Thanks for the opportunity to speak. I’m a nonhierarchal, market-based, non-Libertarian, Silicon Valley kind of guy.

I’m not actually going to talk about the future. I think George did a very nice job. I want to talk about the present and describe a few things that we can do so we try to be better problem solvers.

And just to give a little context. I am a lawyer. I graduated from law school about thirty years ago but spent the majority of my life in and around Silicon Valley. So relative to most people in Silicon Valley, I think I have a pretty reasonable grounding in law, and even the world of federal judges.


\textsuperscript{233} \textit{See} FED. R. EVID. 803(6) advisory committee’s notes.
Relative to most people in law, I have a sort of firsthand experience in Silicon Valley. I was both a customer of Frank Quattrone, and I went to law school with Eliot Spitzer. So that kind of grounds it for you.

So, you know, giving as they would say a hat tip to our local boy Longfellow, I think the danger—and you guys frankly have far, far exceeded my expectations in terms of the level of sophistication—you obviously know way more about all this stuff than I do. But the danger—you remember your Longfellow—is “ships passing in the night.”

So the danger is, we have two systems: the world of the federal courts, which is a beautiful, elegant, hundreds of years old, well-constructed system, and the world of technology, we’ll call metaphorically, Silicon Valley. And those are ships passing in the night.

And that’s a very, very perilous thing. So when I hear somebody go, “Well, I don’t have to know what PowerPoint is,” I’m like, “Bro, you don’t have to know what electricity is either, but it’s part of the world. So you might as well not denigrate it if you don’t understand it.”

In the real world, ships are no longer passing in the night; everybody’s got these systems of integrated information that allow them to keep track of each other, even in the dark. It’s a networked world. It’s a world of ubiquitous connectivity.

I’m fifty-five. I’m probably the median age of people in this room. For most of us, this new world is both empowering and disquieting. No one could possibly say it’s all to the good, but it ain’t going away. So we might as well figure out how to make it work.

And in particular, if we want to stay a world of the rule of law, if we want the U.S. judicial system to remain the most respected system in the United States and around the world, we just can’t say, “I don’t have to understand what electricity is,” that’s not really putting on the big-boy pants or whatever the other analogue would be.

So I went to see a friend of Judge Woodcock the other day, just to give you a sense of reality. Very sharp guy, works for a contract lawyer company.

I walked in the office, and they were all laughing. They were just giggling. I said, “What are you guys so happy about?” They said, “We just got an order for 300 lawyers. We just got an order for 300 lawyers.”

Now, most likely somebody in this room pushed the button on some company through some law firm, which then turned around to hire 300 contract lawyers. But none of us, none of us, even the youngest people in this room, contemplated a world where somebody gets an order for 300 lawyers. And those people have to sit in a room for months analyzing documents in a very jumbly way that has precious little to do with rule of law or access to justice.

The world we’re in is not the world we’re prepared for. So how do we prepare better? Most of the structure of knowledge, including, many people would say, the Bible, is network based, distributed, created over time.
Many of you are familiar with *The Professor and the Madman* by Simon Winchester.234

So name a system created by a small distributed group of people with no competency test who make rules that affect hundreds of millions of people and for which their principal qualification might be—yes, it’s being a politician’s friend. OK.

MR. JOSEPH: Not going to answer that.

PROFESSOR CAPRA: Not for the record.

MR. LIPPE: Not for the record. So *Bowers v. Hardwick*,235 a highly competent decision, but it’s no longer the law because,236 you know, the politics changed. So that’s life. We don’t denigrate the judicial system because the judicial system yielded *Bowers v. Hardwick*. Some people think it was a mistake. Some people think it was a mistake to change it, but it’s part of the system. That can happen.

So how do we think about understanding complex systems from a judicial perspective where there are discrete systems. The judicial system is a complex system, but as George talked about, these technology systems, these networked systems are extremely complex.

And I would suggest having been somewhat in the mix here that most of the failures that we’re seeing, particularly now I’m involved in the banking world a little bit, are failures of complexity.

In law, we tend to approach things as problems of narrative. You’re the bad guy, someone else is the good guy, I’m not the bad guy. That’s the narrative.

I’m sure the world is full of bad guys. But most of these organizational problems are much more problems with complexity than, you know, pick a bad guy. Citibank can no more easily deal with having 100 million emails than any of us could have. So we’re dealing with these problems of complexity. The evidence system is a profoundly interesting accumulation of cognitive wisdom for 800 years about how to interpret stuff. So anyone coming from outside law who spent a couple hours understanding rules of evidence would recognize that it is a very robust, thoughtful system. You guys did a great job.

And anybody who heard any of the discussion today would say, “Oh, that’s really a thoughtful, serious way to approach it.” But anybody from that other world I’m in would be shocked at a comment I’ve heard, that “we don’t ask law students to understand how technology works.”

Well, why wouldn’t we ask law students to understand how technology works? Why wouldn’t we make ever more rigorous attempts to understand how these things work?

So the other thing I’d suggest to you is that there’s kind of two models of change at play. I won’t go too detailed. But our basic model is a

---

Constitutional Convention model: We get all the stakeholders in the room. We debate. We discuss. Majority, super majority, make a decision. Everybody follows it. That’s a great model. That’s not how people stop smoking. That’s not how people started using iPhones. That’s not how most change happens in the world.

Most of the changes you’re talking about, even practice changes within the Justice Department, are changes of practice that happen virally. How do we have a more effective approach to change management?

So this is not a commercial. It’s just an offer. One of the things we’ve done at Legal OnRamp is to create a network of law schools, exactly what George called a network of minds. And we have created large-scale—“we” being sort of me and my general counsel buddy friends—networks of recent law grads to address highly complex problems for big organizations.

And so we’re talking yesterday, they said, “Where are you going?” I said, “I’m going to go talk to a roomful of judges.” They said, “Wait, are you going to get an order?” I don’t think so. Not your kind of order, the kind of order that we care about.

But they said, “Well, let’s do something fun for the judges.” So I said, “Sure, let’s do something fun for the judges.” This is what they do most of the time is, they map contracts in the same way that Richard maps faces, and the same way that you guys map or classify pieces of information under the Rules of Evidence.

So they said, “Let’s start mapping some of this eHearsay stuff.” So they created kind of a mini Wikipedia around these resources. These are all recent grads, Ohio State, Northeastern, B.C.

And then this morning, I said, “Well, there’s something about the iPad, judge. See if you can find something there.” So boom, now they have a whole little section.

So I would tell you that there’s a desperate need from the point of view of the profession generally to create bridge to practice for law schools and for young lawyers. And in the particular case of this topic, there’s a bunch of young lawyers who would be happy to create more resources for you if that were of interest.

But broadly speaking, we all have the opportunity, and I would say the need to understand how these worlds work together; otherwise, we will be ships passing in the night.

And, from time to time, there will be another order for 300 lawyers, which is great, but doesn’t actually solve the world’s problems. So thank you very much.

---

237. See David J. Parnell, Paul Lippe of Legal OnRamp: Every Legal Department Will Seek to “Cisco-ify” Themselves, FORBES (Apr. 4, 2014, 11:50 AM), http://www.forbes.com/sites/davidparnell/2014/04/21/paul-lippe-of-legal-onramp-on-the-legal-market-david-parnell/ (“If there were a Google Maps for the legal market, it would look like Legal OnRamp . . . , a Silicon Valley company that’s partnered with Cisco Systems and different law firms to help legal departments ‘map’ their work product—contracts for instance—through large-scale online collaboration.”).
PROFESSOR CAPRA: Thank you. I now call on Judge Fitzwater to conclude the proceedings.

JUDGE FITZWATER: This symposium has been enormously successful, more successful than I had imagined. I want to begin by thanking our Reporter, Professor Dan Capra, for arranging it and for assembling such a tremendous panel of experts.

As I was listening to this, I was thinking about 1776 and 1787 when lawyers were writing the Declaration of Independence and the Constitution. Physicians were attaching leeches to people and bleeding people. And today, we would say the medical profession has advanced tremendously. The two great learned professions, medicine and law.

It tells me that for law to continue to advance, we must embrace technology, understand technology, and integrate it within our rules and our processes.

And so this conference has been very helpful as part of that process. I thank each of you for coming.
APPENDIX I.

Proper Use of Rules 901, 104(a) and 104(b) in Handling Challenges to Authentication of Electronic Evidence

Paul W. Grimm
District Judge
United States District Court for the District of Maryland

Operative Rules

- Rule 901(a): Requirement of Authentication/Identification
- Rule 901(b): Ten non-exclusive methods of Authentication
- Rule 104(a): Preliminary Rulings by the Court
- Rule 104(b): Relevance Conditioned on Fact

901(a)

- "To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is"
- Level of proof: Preponderance
- Low threshold
901(b)

- Ten non-exclusive methods of authentication, often requiring extrinsic evidence
- Most prominent for use with electronic evidence are:
  - 901(b)(1): Witness with personal knowledge
  - 901(b)(3): Comparison by expert or finder of fact (known authenticity compared to questioned authenticity)
  - 901(b)(4): Distinctive characteristics and totality of circumstances (circumstantial evidence)
  - 901(b)(9): System or process capable of producing reliable results

104(a) & (b): preliminary matters in general, and conditional relevance

- Important rules that interrelate and govern the allocation of the role of judge and jury with regard to authentication of evidence. These rules can be especially important in challenges to authenticity of electronic evidence.

104(a)

- "The court must decide any preliminary question about whether a witness is qualified, a privilege exists or evidence is admissible."
- "In so deciding, the court is not bound by evidence rules, except those on privilege."
- Use of leading questions, hearsay, to lay foundation for admissibility of evidence, including authentication.
- See also 1103(d)(1): The rules of evidence, except for privilege, do not apply to "the court's determination, under Rule 104(a), on a preliminary question of fact governing admissibility."
104(b)

- "When the relevance of evidence depends on whether a fact exists, proof must be introduced sufficient to support a finding that the fact does exist. The court may admit the proposed evidence on the condition that the proof be introduced later."

- Potentially important rule when electronic evidence is offered, especially social media and similar evidence that is susceptible to being altered, "spooled" or fabricated.

- Implicated when there are plausible facts supporting a finding by a reasonable jury that the evidence is authentic, as well as a finding that it is not authentic.

- When implicated, the court does NOT make final decision regarding admissibility; the jury does.

- Court instructs jury regarding their options.

The Battlefield: the Maryland approach vs the Texas/Delaware Approach

- Griffin v. State, 194 Ar 415 (Md. 2011): Reversed trial court’s admitting MySpace page from girlfriend of defendant because trial judge “failed to acknowledge the possibility of likelihood that another user could have created the profile . . . or authored [the threat],” despite absence of evidence that anyone other than girlfriend created the page, and despite abundance of characteristics linking the page to the girlfriend.

Texas/Delaware Approach

- Thunda v. State, 358 S.W. 3d 635 (Tex. Crim. App. 2012): Affirmed admission of MySpace evidence despite defense evidence that it is easy to fabricate a social media posting (but no evidence that this actually had happened), because of the abundance of circumstantial evidence supporting inference that defendant made the post. Opinion did not discuss 104(a) or (b) issues, only authentication rules. Rejected Griffin approach.

APPENDIX II.

Rule 901(b)(11) — Email

(11) Evidence About an Email Communication.

For an email communication, evidence that an email

**hearing the customary format** of an email, including

the email address of the sender and recipient:

**(A)** was sent to the email address assigned at the
time to a particular person, if circumstances, which
may include some or all of the following, show

that the person received the email.
Rule 901(b)(11) — Email

i. A reply to the email was received from the email address assigned to the person;

ii. Subsequent communications with the person reflect the person’s knowledge of the contents of the email;

iii. Subsequent conduct of the person reflects the person’s knowledge of the contents of the email; or

iv. The person produced the email in the action.

(B) was received from the email address assigned at the time to a particular person, if circumstances, which may include some or all of the following, show that the person sent the email:

i. The email contained the typewritten name or nickname of the recipient or the sender in the body of the email;

ii. The email contained the signature block or electronic signature of the person;

iii. The contents of the email would normally be known only to the person or to a discrete number or category of people including the person;

iv. Subsequent communications with the person reflect the person’s knowledge of the contents of the email;

v. Subsequent conduct of the person reflects the person’s knowledge of the contents of the email; or

vi. The person produced the email in the action.
Rule 901(b)(12) — Website Contents

(12) Evidence About Website Contents. For a webpage from the website of a business, public office or other organization (regularly conducted activity), a printout or other output readable by sight bearing the Internet address and the date and time the webpage was accessed and the contents of the exhibit downloaded, provided that:

Rule 901(b)(12) — Website Contents

(A) A witness testifies or certifies in compliance with a federal statute or a rule prescribed by the Supreme Court that:

i. The witness typed in the Internet address reflected on the exhibit on the date and at the time stated;

ii. The witness logged onto the website and reviewed its contents;

iii. The exhibit fairly and accurately reflects what the witness perceived; and

Rule 901(b)(12) — Website Contents

(B) The exhibit bears indicia of reliability, which may include:

i. Distinctive website design, logos, photos or other images associated with the website or its owner;

ii. That the contents of the webpage are of a type ordinarily posted on that website or websites of similar entities;

iii. That the contents of the webpage remain on the website for the court to verify;
Rule 901(b)(12) — Website Contents

iv. That the owner of the website has elsewhere published the same contents, in whole or in part;
v. That the contents of the webpage have been republished elsewhere and attributed to the website;
vi. The length of time the contents were posted on the website; and

Rule 901(b)(12) — Website Contents

(C) Before the trial or hearing, the proponent gives an adverse party reasonable written notice of the intent to offer the webpage so that the party has a fair opportunity to challenge it.

Rule 902(13) — Self-Authentication of Email

(13) Email. The email bears the customary format of an email and purports to issue from the email system of a business, public office or other organization (regularly conducted activity) and not from a public email system. Before the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the email so that the party has a fair opportunity to challenge it.
Rule 902(14) — Self-Authentication of Texts

(14) Text Message. The text message bears the customary format of a text message and purports to emanate from a number or other unique source designation assigned at the time to a particular device. Before the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the text message so that the party has a fair opportunity to challenge it.

Electronic Evidence Symposium
Advisory Committee on the Federal Rules of Evidence
April 4, 2014

Authentication: Rule Possibilities

Gregory P. Joseph
Evidentiary Rules for Electronic Evidence:

Two Proposals

John Haried, Assistant U.S. Attorney
Chair, eDiscovery Working Group
EOUSA – U.S. Department of Justice

Disclaimer

Neither of my proposals is an official proposal of the U.S. Department of Justice at this time.

Both proposals are merely preliminary thoughts for discussion.

Proposal #1:

The rules of evidence should permit an out-of-court certification of authenticity for machine-generated information that can be authenticated under Rule 901(9) and that is similar to a business record.
Authenticate Evidence – Rule 901(9):
Evidence About a Process or System. Evidence describing a process or system and showing that it produces an accurate result.

What’s the hole in the current Rules?

Certifications
902(11): Certified Domestic Records of a Regularly Conducted Activity
902(12): Certified Foreign Records of a Regularly Conducted Activity
902(13) – reliable machine-generated information under Rule 901(9)?
Under heading “United States”

Military and intelligence

- The SDS
  - OPLAN/CONPLAN REG, 2003 revision.
  - OPLAN/CONPLAN REG, 2007 revision.
- CIA database interrogation sites. While the CIA claims to have destroyed 40 of the videos, others are known to remain.
- The US “Saba Dugout” from image collections, with intact images, hopefully unmodified and explained.
- Database shown publicly with the Obama administration.
- Wasting program led by CIA.
- Brief correspondence between the National Security Agency and Amstronics companies such as AT&T, Verizon, and Qwest, regarding the warrantless wasting program. Correspondence involving individuals who participated with the

Cases on authenticating Wayback Machine screen captures

7. Audi AG and Volkswagen of America v. ShokanCoachWorks, Inc., 392 F.Supp.2d 246, 278 (N.D. New York 2008) (Defendants correctly point out that the Adams Declaration cannot authenticate the search results from www.archive.org because such evidence may only be authenticated by a knowledgeable employee of the website.).

3. PE 109 for ID is not sufficiently credible to be a self-authenticating business record (AW MRE 595(11) and MRE 100(6)). For authentication (MRE 595(4),) federal case law on the authentication issue is persuasive. A witness testifying the admission of archived websites must either have knowledge of the archiving procedure used by the archiving entity and that party donor entity such that the witnesses can readily tell the archive accurately shows true copies of the websites as purport to archive at must have knowledge of the original webpage consistent with the witness can verify that the archived copy is true copy of the original. The Government has insisted the Court that it does not intend to admit the statement of David G. Skidmore (Government’s brief). Accordingly, this court finds that the Government has not properly authenticated PE 109 for ID and it is not admitted.
6. PE 109 for ID is a request for information and is offered for the fact that the request was made not for the truth of the matter asserted. The Government offers PE 109 for ID for a non-hearsay purpose as circumstantial evidence that PFC Manning was aware of PE 109 for ID and his intent to gather information and send it to WikiLeaks. Although the Government has not presented evidence that the accused actually accessed PE 109 for ID, the Government has presented evidence that PFC Manning searched Internets for WikiLeaks and for some of the information on PE 109 for ID. The Government also

So ORDERED this 28th day of June 2013.

DENISE R. LIND
COL., JA
Chief Judge, 1st Judicial Circuit.

What happened in the Manning trial?

Proposed Rule 902(13)

Certified Records of Regularly Conducted Activities Generated by a Machine. The original or a copy of a record if:

(A) the record was generated at or near the time by a machine utilizing a process or system that produces an accurate result;

(B) the record meets the requirements of Rule 803(6)(B), (C), and (E);

(C) as shown by a certification that meets the certification requirements of Rule 902(11) for domestic records or Rule 902(12) for foreign records.

The proponent must also meet the notice requirements of Rule 902(11).
Proposal #2:
The Rules of Evidence should permit a certification to authenticate a copy of an electronic device, media or file by its “hash function” or other reliable method.

Certifications
902(11): Certified Domestic Records of a Regularly Conducted Activity
902(12): Certified Foreign Records of a Regularly Conducted Activity
902(13) – reliable machine-generated information?
902(14) – identical copies of electronic devices, media, files?

What is a “hash function”?
- A hash function is any algorithm that maps data of arbitrary length to data of a fixed length. The values returned by a hash function are called hash values, hash codes, hash sums, checksums, or simply hashes.
Routine uses of hash functions

- Removing duplicate emails from a large collection of emails.
- Verifying the integrity of a file that has been transmitted electronically.

When do copies need to be authenticated?

Seized evidence → Analysis for court

Data set #1: Original data

"We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America."

MD5: 26a981554d7d761230bc7ef3a6645375
SHA-1: f15b1ce9a37e7fb69086f25216617ae0a9e5706e
Data set #2: period omitted

"We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America."

MDS: 8ef46ff929b2b1af43f7bb326562ecc1
SHA-1: 37e8bbd169beb75c446db1ad844e82b7aea9b68f

Data set #3: space added

"We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America."

MDS: 7d522bbe8e38a6da208acad47503419f
SHA-1: e8bf83af375a42581e30cb94d4c2773be9874c71
APPENDIX IV.

Proposed Rule 902(14)

Certified Copy of Electronic Device, Storage Media or File. A true and accurate copy of an electronic device, storage media or file is:
(A) the copy is true and accurate as shown by a reasonable means; and
(B) the record meets the requirements of Rule 803(6)(E);
(C) as shown by a certification that meets the certification requirements of Rule 902(11) for domestic records or Rule 902(12) for foreign records.
The proponent must also meet the notice requirements of Rule 902(11).

Authenticating Digital & Multimedia Evidence: Can Biometrics Play a Role?

Dr. Richard Vorder Bruegge
Senior Photographer Technologist, FBI OTD TASB

Advisory Committee on Evidence Rules Symposium on the Challenges of Electronic Evidence
Friday, April 4, 2014
University of Maine School of Law, Washburn Lee Auditorium
DISCLAIMER #1

The text presented herein, along with the views and opinions expressed in the course of this presentation represent those of the speaker alone, and do not necessarily represent those of the Federal Bureau of Investigation, the Department of Justice, or the United States government.

Integrity vs. Authenticity

“The King’s Scroll”

INTEGRITY – Is the content complete and unaltered? (“Seal”)

AUTHENTICITY – Does the content truly represent what it purports to represent? (“Signature”)

“...is a true and accurate depiction...”

_integrity is often (but not always) a component of Authenticity

“...is a true and accurate depiction...” for CCTV evidence.

For Digital Evidence, Integrity may be considered as “solved”

- Binary hashes (e.g., MD-5, SHA-256) are “Gold Standard”

Biometrics

DEFINITION: Biometrics are the measurable biological (anatomical and physiological) or behavioral characteristics used for identification of an individual.

Anatomical (only):
- DNA
- Fingerprint (e.g., finger, palm,...)
- Face
- Iris
- Vascular Patterns (e.g., hand, finger, toe...?)

Behavioral (and Anatomical...):
- Voice/speaker
- Gait
- Handwriting/signature (dynamic?)

Note: The list above is not an exhaustive list, but merely represents some of the most common
"Ideal" Characteristics of Biometric Signatures

- Persistent Over Lifetime
  - Infant to Senior
- Extremely High Ability to Individualize
  - > 7 Billion people on Earth
- Easy & Low Cost to Use/Implement
  & People are willing to use..."Most important?"
- Extremely Difficult to Spoof
  & Can be kept Private?

Suitability of Modalities for Authentication

DISCLAIMER #2

Assess how well different biometric modalities meet the "ideal" criteria, within the context of their use for authentication of digital and multimedia evidence in legal proceedings.

Handwritten Signatures are not "Ideal"

- Not Persistent Over Lifetime
- Individualize for >7B people?
- Easy to use, but also to Spoof (when static)
  - Forger
  - "Cut-and-paste"
- What about other modalities?
<table>
<thead>
<tr>
<th>DNA?</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Persistent Over Lifetime</td>
</tr>
<tr>
<td>▪ Individualize for 7B+ people</td>
</tr>
<tr>
<td>▪ Costly, Slow, and...</td>
</tr>
<tr>
<td>▪ User acceptance?</td>
</tr>
<tr>
<td>▪ Hard to spoof</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Friction Ridge?</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Persistent Over Lifetime</td>
</tr>
<tr>
<td>▪ Individualize for 7B+ people</td>
</tr>
<tr>
<td>▪ Requires more sampling</td>
</tr>
<tr>
<td>▪ Easy to Use</td>
</tr>
<tr>
<td>▪ Disney</td>
</tr>
<tr>
<td>▪ Hard to spoof</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Challenges with other Biometric Modalities</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Relatively low persistence over long time</td>
</tr>
<tr>
<td>▪ Individualizing for 7B+ requires more sampling</td>
</tr>
<tr>
<td>▪ Easy to use</td>
</tr>
<tr>
<td>▪ Not private and easy to spoof</td>
</tr>
<tr>
<td>▪ Iris?</td>
</tr>
<tr>
<td>▪ Seems to be persistent over time (though there is some debate)</td>
</tr>
<tr>
<td>▪ Individualizing for 7B+ requires more sampling</td>
</tr>
<tr>
<td>▪ Easy to use</td>
</tr>
<tr>
<td>▪ Not private, but hard to spoof</td>
</tr>
</tbody>
</table>
Implementing Biometric Authentication

- There will be challenges to creating any system to authenticate digital and multimedia evidence.
- No known implementations for authentication of evidence through biometrics, but they are probably better than handwriting.
- Friction ridge and iris offer best option for near term.

Implementing Biometric Authentication

- Before accepting such an approach, however, extensive Test and Evaluation will be critical.
- Binary Hashing can Assure Integrity, but must append a biometric template to data if that is authentication.
- Technology exists to wrap digital signatures (or "biometric templates"), but must have an integrated system.
APPENDIX V.

eHearsay
A (not so) New Exception for a New Kind of Evidence?

Jeffrey Bellin
William & Mary Law School
bebll@wm.edu
Twitter: @jbebllin

Electronic Out-of-Court Statements

- text messages
- social media (Facebook, Twitter)
- email
- instant messaging/chats

General Attributes

- Narrate Recent Phenomena
- Communicate w/ Friends prior to Controversy
- Frozen in Time – time/date + recipient/sender
- Overcome Memory Loss/Non-Cooperation

Describes Recent Events
Pre-Litigation Communication
Recorded
Declarant Unavailable or Testifies

A Hearsay Exception Whose Time Has Come?

Thayer (1896)
- made in writing
- ante litem motam
- deceased declarant
- personal knowledge

Uniform Rule 65(a)(1) (1955)
- recently perceived event
- recollection clear
- prior to commencement of the action
- declarant unavailable (or testifies)*
- made in good faith

eHearsay (RSRP)
- recorded communication
- recently perceived event
- not in contemplation of litigation
- declarant unavailable or testifies
- not anonymous

FRE 804(b)(3) (SRP) (1996)
- recently perceived event
- clear recollection
- not in contemplation of litigation
- in which interested
- declarant unavailable
- made in good faith
Rule 806. Exceptions to the Rule Against Hearsay—When the Declarant Is Unavailable as a Witness:

1. The following are not excluded by the rule against hearsay if the declarant is unavailable as a witness:

2. Recorded Statement of Recent Perception. A recorded communication that describes or explains an event or condition recently perceived by the declarant, but not including: (a) a statement made in contemplation of litigation, or to a person who is investigating, litigating, or settling a potential or existing claim; or (b) an anonymous statement.

Rule 801... Exclusions from Hearsay

. . . (6) A statement that meets the following conditions is not hearsay:

1. The declarant testifies and is subject to cross-examination about a prior statement, and the statement...
## APPENDIX VI.

### UNAVAILABILITY RECENT PERCEPTION EXCEPTION

<table>
<thead>
<tr>
<th>Unavailability</th>
<th>Recent Perception</th>
<th>Written</th>
<th>Oral</th>
<th>Not in Shadow of Legality</th>
<th>Grounds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Driver’s Death</td>
<td>Yes***</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Medical Evidence Act of 1990</td>
<td>Yes**</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Goodheath Landmark</td>
<td>Yes**</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Unnamed Rule (1900)</td>
<td>Yes**</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Wyoming Fed. R. Code (1931)</td>
<td>Yes**</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Professional Behavior</td>
<td>Yes**</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

*Civil cases only.
**The declarant must be deceased.
***Limited to "necessity cases."
****Writing must not be "anonymous."

---

### 3. Hawaii Hypothetical

**A. Unavailable Deponent**

V is on trial for the murder of W. Consider the admissibility of the following:

1. A text message from V to her close friend the day before the murder. "If I can’t do it yesterday and determined to return and finish the job."

2. An email message sent by V to P, please don’t believe any other case as #1.

3. An oral statement from V to W, but otherwise some case as #1.

4. Same as #1 but P took and remembered some case of V’s oral statement.

5. A diary entry by V, but otherwise some case as #1.

6. Same as #1 but with this addition. "If anything happens to me give this text to the police."

7. Same as #1 but V and P are engaged in a later custody dispute.

8. An anonymous text to V’s mother. "I am present myself to take care of V’s needs. Protection. I can’t disclose my identity. Too scared." The identity of the text cannot be determined.

9. Same as #1, but the identity of the text is determined and the text is new. dead.

**B. Available Deponent**

V testifies in her neighbor. "If I can’t do it myself, I will do it myself. I want to take care of anyone. Can you come take me to the hospital?" As D’s trial for assault, V testifies, and denies that D assaulted her, claiming that she fell. Is the text admissible as substantive evidence? What is the text admissible as substantive evidence? What if instead V were a diary entry (or hours later describing the incident)?
APPENDIX VII.

The Evidentiary Adverse Inference Instruction

April 4, 2014
Presented by Shira A. Scheindlin
United States District Judge
Southern District of New York
The New Proposed Rule 37(e)

1. If party fails to preserve electronically stored information that should have been preserved in the ordinary course of business, the court may:
   a. Order the party to produce information that would otherwise be discoverable, and if the party does not comply, the court may take such other remedial action as is appropriate, including holding the party in contempt of court.
   b. Issue a protective order against disclosure of the information.
   c. Award reasonable costs, including fees, to the party or nonparty entitled to the information.
2. In determining the appropriate relief, the court should consider:
   a. The prejudice that the non-preservation of the information has caused the party.
   b. Whether the party had notice of the importance of the information.
   c. Whether the party had an adequate opportunity to preserve the information.
   d. Whether the non-preservation was intentional or innocent.

Jury Instruction

In this case, evidence has been received which the Defendant contends shows that a photograph exists or existed of the upstairs of what had been referred to as the barn house, but no such photograph has been produced. If you find that the Defendant has proven by a preponderance of the evidence, one, that this photograph exists or existed, two, that the photograph was in the exclusive possession of the Plaintiff, and, three, that the non-production of the photograph has not been satisfactorily explained, then you may infer, though you are not required to do so, that if the photograph had been produced in court, it would have been unfavorable to the Plaintiff. You may give any such inference, whatever force or effect as you think is appropriate under all the facts and circumstances.” 720 F.2d 387 (9th Cir. 1983) (emphasis added).

37(e) Advisory Committee Notes

“Subdivision (e)(1) applies to jury instructions that permit or require the jury to infer that lost information was unfavorable to the plaintiff or other party. Subdivision (e)(2) covers any instruction that directs or permits the jury to infer from the loss of information that the information was in fact unfavorable to the party that lost it. The subdivision does not apply to inferences that may be drawn from evidence introduced during a trial or jury instructions that do not involve such an inference. It is not intended to prohibit a court, in an appropriate case, from allowing the parties to present evidence and argument to the jury concerning the loss of information. Nor would it bar a court from instructing a jury that it may determine from evidence presented during the trial whether lost information was favorable or unfavorable to positions in the litigation. These measures would be available under subdivision (e)(1) if no greater than necessary to cure prejudice.” Committee Note, Discovery Subcommittee Report Rule 37(e) at 22 (emphasis added).
Sample Jury Instruction

"If you find from all of the evidence admitted during the trial that a party has lost or destroyed information relevant to the issue that should have been preserved, and the loss or destruction has not been adequately explained, you may—but need not—infer that the information would have been unfavorable to the party who lost or destroyed it."

Proposed Evidentiary Rule

(a) Prima Facie Showing. To make a prima facie showing for a presumptive adverse inference instruction, the moving party must demonstrate (1) a preservation of the evidence that the opposing party (2) lost or destroyed relevant evidence, if within that party’s control, (3) as to which the movant is able to preserve at the time of the loss or destruction.

(b) Presumption. The non-moving party may negate a prima facie showing by demonstrating by a preponderance of the evidence that (1) the lost or destroyed evidence would not have been beneficial to the moving party’s case, or (2) a substitute replacement to the lost or destroyed evidence is available.

(c) Burden of Proof. If the non-moving party cannot demonstrate both of paragraph (2) above, then the burden shifts to the moving party to affirmatively demonstrate prejudice as defined in (3).

(d) Balancing Test. If the moving party carries its burden, the circumstances of destruction and the likely contents of the missing evidence shall be decided by the jury pursuant to a presumptive adverse inference instruction, unless the judge finds that prejudice to the non-moving party significantly outweighs the benefit of the instruction to the moving party.

(e) Definitions. A presumptive adverse inference jury instruction is one that infers no fault or wrongdoing by the alleged offender, but rather simply that the party in fact failed to preserve the information it should have been expected to preserve, regardless of the circumstances of destruction and the likely contents of the evidence, and to accord that inference whatever weight it deemed appropriate.
APPENDIX VIII.

**DOES DAUBERT APPLY TO CHALLENGES TO COMPUTER-ASSISTED REVIEW OF ELECTRONICALLY STORED INFORMATION?**

Daniel K. Gelb, Esquire
GELB & GELB LLP
84 State Street
Boston, MA 02109
(617) 345-6010 (T)
(617) 345-6009 (F)
dgelb@gelbgelb.com
www.gelbgelb.com

The Sedona Conference®:
Search and Information Retrieval
(Practice Point 7)

"...[p]arties should expect that their choice of search methodology will need to be explained, either formally or informally, in subsequent legal contexts (including in depositions, evidentiary proceedings, and trials)."

**COMPUTER ASSISTED REVIEW**

- Keyword search terms
- De-duplication/near-duplication of documents (e.g., reducing redundant email threads, etc.).
- Predictive Coding
Fed. R. Evid. 702

A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:

a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;

b) the testimony is based on sufficient facts or data;

c) the testimony is the product of reliable principles and methods; and

d) the expert has reliably applied the principles and methods to the facts of the case.


- The judge is the "gatekeeper" who determines whether expert testimony is "relevant to the task at hand" and that it rests "on a reliable foundation."
- The judge must determine if the expert testimony is "reliable" and if it has "scientific validity." The judge should ask if the testimony is "based on scientifically valid methods, and whether the results are capable of being reliably produced in the context of the case at issue." This inquiry involves the following factors:
  1) Empirically tested?
  2) Subject to peer review/publication?
  3) Known and/or potential rate?
  4) Operational standards/controls?
  5) Generally accepted by the relevant scientific community?

Predictive Coding

- Differing perspectives on how to best develop "seed sets" against which to test the particular technology (i.e., sampling):
  - Some believe the most representative set is a completely randomized sample without the software having conceptual "knowledge" of the data set.
  - Alternate approach is "teaching" the software specific concepts using criteria from metadata or search term results.
  - Hybrid approach—depending on technology used.
Emerging Litigation Surrounding Predictive Coding / Computer Assisted Review

- EORHB, Inc. v. HOA Holdings, LLC, CIV.A. 7409-VCL, 2013 WL 1900621 (Del. Ch., May 6, 2013)
- In Re: Actos (Pioglitazone) Products Liability Litigation, MDL No. 6:11-md-2299 (July 27, 2012) (Trial Order)

Differing Perspectives on the Applicability of Daubert Predicates to E-Discovery Review

- Equity Analytics, LLC v. Lusardi, 248 F.R.D. 331 (D.D.C. 2008) ("Determining whether a particular search methodology, such as keywords, will or will not be effective certainly requires knowledge beyond the ken of a lay person (and a lay lawyer) and requires expert testimony that meets the requirements of Rule 702 of the Federal Rules of Evidence.")
- Victor Stanley, Inc. v. Creative Pipe, Inc., 250 F.R.D. 251 (D. Md. 2008) ("...challenges to search and review methods, such as keyword-based searches, involve technical and scientific subjects...")

Question #1:
Can Daubert Apply to Computer Assisted Review?

- FRE 702(a):
  
  
  "...the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue..."

  
  
  Daubert is not procedurally ripe unless the the fact-finder will be presented an evidentiary question.

  
  
  In other words, the, but what procedural mechanism do litigants have to raise this if Daubert and 702 is relegated to the fact finding process and not reliability of discovery methods?
Question #2: Should Daubert Apply to Computer Assisted Review?

- The type and volume of ESI differ across litigations—both civil and criminal.

- The Advisory Committee’s Notes on the 2006 amendments to Fed. R. Civ. P. 26(f) exemplify why parties are not to approach e-discovery as a perfunctory task:

  ...it may be important for the parties to discuss these systems, and accordingly important for counsel to become familiar with those systems before the conference. With that information, the parties can develop a discovery plan that takes into account the capabilities of their computer systems. In appropriate cases identification of, and early discovery from, individuals with special knowledge of a party’s computer systems may be helpful.

Question #2: Should Daubert Apply to Computer Assisted Review? (cont.)

- Is the TAR product used verified and tested?

- Computer assisted review is based on science with customized processes derived from, among other disciplines, statistical analysis.

Question #2: Should Daubert Apply to Computer Assisted Review? (cont.)

- Fed. R. Evid. 102: “These rules should be construed so as to administer every proceeding fairly, eliminate unjustifiable expense and delay, and promote the development of evidence law, to the end of ascertaining the truth and securing a just determination.”

- The stakes for litigants are too high for a finding not to be made on the reliability of the technology, including verification of the standard operating procedures used and module(s) subject to challenge.

- TAR, if not implemented properly or tested, risks false/incomplete results that could compromise a litigant’s claims or defense at trial (e.g., patterns or quantity of particular types of documents with relevant content, custodians/chain of custody; knowledge/intent, etc.)