

All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

The evidence please

I have been watching a lot of information about the Trump impeachment process, reading much of the content, and occasionally posting things I consider to be important for others to read on our Web site. I have also worked in digital forensics for, something like 30 years now.

The thing I notice most among the political class is their desire for narrative over evidence. The same is true for sales and marketing in the broader sense, and of course it makes perfect sense. Propaganda is more effective than facts at convincing people to do what you want them to do. But it comes to extremes at times.

No predictions

I don't mind prognostications, although I find many of them to be ridiculous. I am not going to predict what will happen, but I think it is worth thinking a bit about what might happen. As I write this, the US Senate is just starting to take the oath, and I hope the Chief Justice requires that the jurors not discuss the case with each other or anyone else and not watch any other coverage or get information on the case from any other source... No way this is going to happen, but that's how it is in every other trial.

I suspect there will be no forensic evidence presented. This tends to be boring (or so I am told – but maybe it's just my testimony that tends to be so). This, to me, is the biggest problem we face in coming to clarity and just decision-making.

Really? Forensic evidence? At an impeachment?

Here's the thing. Suppose we see evidence that includes emails, text messages, social media posts, video recordings, pictures of hand written notes, etc.

If I were on the defendant's side, I would:

- Claim the evidence is all fake – the fake news – the fake emails – the fake text, etc.
- Claim some of my own evidence – newly found – from some other source.

We just recently heard about the Russians breaking into the computers in a Ukrainian company – and the news kept talking about leaking secrets or internal emails or whatever. But they ignored the propagandist approach of introducing your own fake digital documents and then leaking them “legitimately”.

Now we have two scenarios, the waters are muddied, and the two sides go to their publics' and claim the other is lying. How do we as the public sort this all out?

Forensics and Expert Witnesses!!

Here's what I think should (always) happen. Each side should have forensic experts with proper expertise (knowledge, skills, training, education, and experience) testify as to the provenance of any documentary evidence. This includes such evidence as may be identified by eye witnesses, because eye witness accounts are notoriously problematic and the expert forensic testimony from two sides typically eliminates the obvious biases and corruptions.

But this doesn't just go for impeachments. It goes for all legal proceedings, and frankly, the methods used should be applied to lots of other areas in today's deceptive networking environment.

Consistency analysis

It's all about the consistencies or inconsistencies within and between different traces and claims. Those of you who have read my historical papers in this arena know that I am a big fan of consistency analysis, have published papers on it, and have testified in court about consistencies and inconsistencies within and between evidence and testimony.

- One side claims a "tweet" by the President (or your sister) and the other claims it's a fake. "I never said that" - likely true if they tweeted it – tweeting, despite having the protection of speech in the sense of freedom of, is not in fact oral emanations from a human mouth.
 - The forensics experts (assuming there is such evidence), present the evidence supporting or refuting the claim by showing the provenance (where it came from when, by whom, etc. to the extent it is demonstrated by the evidence and the scientific basis for and against that provenance).
 - They should NOT disagree about the facts or the evidence itself. If they do, one of them is almost certainly not using a valid basis and it should be pretty clear from the details they present.
 - They may disagree about the interpretation of the evidence. Each may have different procedures they applied that indicate consistency or inconsistency with different theories of the case. Real experts almost never disagree about these technical issues when properly litigated.

The details and the presentation of those details by the experts under direct and cross-examination are usually revealing to the jury, and most jurors and juries succeed at setting aside other interests and can accept the reasonable conclusions of the evidence.

What the jury does with that evidence in the context of the rest of the case is, of course, a different matter, and beyond the realm of the forensics experts.

No conclusions about the case

Which brings us to the final comment I have. The pundits and the press who ask them about their views have a strong tendency to try to get a final outcome of the case conclusion from the experts. But courts have a rule about that, and so should the experts.

Conclusions

Real experts, regardless of what they may think themselves, don't draw conclusions about the ultimate outcome of the legal matter. They draw conclusions about the evidence in their areas of expertise. No digital forensics expert can say legitimately that you did anything – or not. They can only really legitimately claim that the evidence is consistent or inconsistent with various theories of what took place. They may say things like "I know of no other way...", or "I don't know of any way ...", but that's not the same as, and miles apart from "There is no way ...".

We the people can indeed handle the facts. Please let us see them and their provenance.