



Center for Legal and Court Technology's Latest Laboratory Trial Tested Whether a Defendant Can Be Convicted Based on Fabricated Computer Evidence

February 20, 2011

Since 1995, the Center for Legal and Court Technology (CLCT) has been conducting nearly annual experimental cases to determine how modern technology can assist in resolution of disputes. CLCT's Laboratory Trials have included a pre-September 11th three continent terrorism case, the world's first known courtroom use of holographic evidence and immersive virtual reality, determination of how to use technology for multi-national alternative dispute resolution, a new protocol for joint trial of a case by courts in multiple countries, and the nation's most sophisticated assistive technology trial.

CLCT's 2010 Lab Trial was designed to examine the degree to which it is possible to successfully fabricate computer evidence and how trial participants, including jurors, are likely to react to such a case tried in a high-technology courtroom. The case, *United States v. Varic*, simulated a federal criminal prosecution in which the primary evidence came from digital sources, such as emails and computer files. Trial was conducted before the Honorable Barbara Rothstein, United States District Judge and Director of the Federal Judicial Center. The witnesses included two experienced FBI forensic computer experts. The case included evidence presentation technology, a multi-media court record, and remote testimony. The defendant was charged with attempted child slavery, and most of the prosecution evidence was in the form of electronic exhibits illustrating the defendant's attempt to entice a 15 year-old girl to travel to the United States to work as a domestic servant for the defendant. Several incriminating emails and portions of files were found on the defendant's computer. The defendant claimed that the incriminating evidence must have been fabricated by a former friend of hers, whom she claimed became furious with her when she rejected his request for money as well as his romantic advances. She alleged that the friend had used her unprotected wireless router to place the incriminating evidence on the computer and had also used other technology, such as a keylogger program, to capture the information necessary to send emails from her computer.

We recruited a twelve person jury designed to demographically model a representative United States jury. For the first time since CLCT began conducting its experimental trials, the October 16th, 2010, Lab Trial concluded with a hung jury. Also of note is that the vote was evenly split – six for conviction and six for acquittal.

The Lab Trial's goals included:

1) Learning to what extent it is now possible to flawlessly fabricate computer evidence, assuming that the fabrication would be the work of a highly talented individual with limited resources.

2) Obtaining insights into how a representative jury may react to significantly technical forensic computer evidence.

3) Ascertaining how well the upgraded 2009-2010 McGlothlin Courtroom would work in a case of this type.

Results:

1) *Fabrication of computer evidence* – During preparation of the case, we learned that in determining whether an email or document found on a computer was drafted by a specific person or originated on a given computer, there can be multiple explanations as to how a document or email or trace of it ends up on a computer. When evaluating who the creator was or whether the computer owner knew of the file, there is no one “smoking gun” that will determine who caused the data to be put on the computer. Instead, investigators must also look for other information that corroborates or conflicts with data found on a computer. We drew two especially important conclusions from the trial. It *is* possible to create convincing false computer evidence that can be extraordinarily difficult to identify and discredit. However, it is also very difficult to discredit defense theories that seek to justify multiple explanations for the existence and form of computer evidence.

2) *Jurors' reactions to technical forensic computer evidence* – Results of a pre-trial questionnaire showed that members of our jury, whose ages ranged from 20 to 76, were already more knowledgeable about computers and email than we had expected. Post-trial questionnaires revealed that most of them were able to understand the testimony of the computer forensic expert witnesses. They did not feel as though the expert witnesses used too much technical jargon, nor did they feel as though the expert witnesses were condescending when explaining the technology. In order for us to be able to finish the trial in one day, the expert witnesses limited their testimony to about one hour each by narrowing the scope of their explanations of computer data storage and transmissions, as well as the methods by which someone can gain access to and control of another's computer. They also discussed only a few of the indicators they would have checked during a forensic examination of a suspect's computer. However, we did note that even with the limited testimony of the experts, there was an indication that several of the jurors must have tuned out for a time or gotten a little confused. So it is likely that if the testimony had taken several days, as it normally would have, we would have lost much more of the jurors' attention. The split verdict was inconclusive in establishing whether the defense adequately injected reasonable doubt in the authenticity of the evidence because during the post-trial discussion, several of the jurors indicated that the reason they voted to acquit was because they were not convinced that the reason the defendant was trying to get a child was in order to have a slave to do housework. CLCT Director Professor Fred Lederer believes that most if not all of the jurors accepted the fabricated evidence as true. As noted, those who would not have convicted did so for other reasons.

3) *Effectiveness of the McGlothlin Courtroom* – The system upgrades to the courtroom worked well. In addition to use of presentation technologies, we used pictures of key witnesses for voir dire; live remote testimony of a witness via a new Cisco (Tandberg) Movi portable video conferencing system; realtime transcription; multi-media court record publication via Internet; and jury room electronic display of the evidence. Both Professor Lederer and the trial judge were impressed by the quality of the remote testimony, and the jurors received that testimony well.

BUT

This experiment suffered from a fundamental problem. It was a simulation, and there was no truth. Not only did we not have a real crime or defendant, we also did not have evidence of a real world event. *We* created the evidentiary exhibits. We did so with highly expert assistance, and we did so with the intent that our situation would duplicate how the evidence would have appeared (or would have responded to forensic computer analysis). From our perspective, we can conclude that it is possible to create false but highly convincing computer evidence because our experts concluded that it likely would have passed forensic muster. However, because our evidence never existed in the real world we must concede that our conclusion is not based on a real case and is therefore questionable.

Conclusions

Subject to the discussion above, we conclude that it is now possible to create sufficiently well-crafted fraudulent electronic evidence able to withstand expert analysis that the risk cannot be dismissed. However, in the real world, the chance of doing so successfully is probably small as the myriad of other forms of data that would have to concur with the evidence is such that inconsistencies probably would be noted. However, there are so many alternative reasons for the existence or absence of many distinguishing electronic data features that the defense in a criminal case has a substantial chance of prevailing by arguing that the prosecution cannot prove its case beyond a reasonable doubt.

Highly knowledgeable forensic computer experts able to explain technology simply and clearly to jurors or judge are critical for both prosecution and defense. The use of evidence presentation technology to visually explicate matters such as how email works can be important.

To be successful, electronic data prosecutions ought to be accompanied by as much traditional corroborating evidence as may be feasible.

Jurors appear able to understand the basic of computer technology and may well have a greater fundamental understanding than accepted. However, in this non-scientifically controlled experiment, we cannot know whether our jury was representative of others.

As previously ascertained, technology enhanced courtrooms assist jurors in understanding evidence, provide means such as videoconferencing for providing evidence not otherwise available, and appear to speed trial along.

More work is necessary, and controlled scientific studies are highly desirable.