There's no code of ethics to govern digital forensics – and we need one

August 10 2015, by John J Sloan, Iii

How to deal with all that digital evidence? Credit: West Midlands Police, CC BY-SA

Let me begin with a disclaimer: I am neither a digital forensics practitioner nor do I play one on television.

I am, however, a professor in, and former chair of, an academic department at a research university that houses a graduate program in computer (digital) forensics I helped design. In 2011, I cofounded a

computer forensics research center at my university. Finally, for more than 10 years, I have taught undergraduate and graduate courses on professional ethics for criminal justice and digital forensics students.

These experiences helped me to identify a glaring issue in the field of digital forensics: a lack of professional and ethical standards governing practitioners. And as digital forensics gains prominence in the legal landscape, the lack of agreed-upon standards is a big problem.

What *is* digital forensics?

Digital or computer forensics involves the identification, recovery, analysis and presentation in court of relevant information taken from electronic devices such as computers and cellphones.

That information becomes digital evidence presented in court and designed to tie together people and events in time and space to establish causality for crimes or civil wrongs.

For example, imagine the police arrested a suspect on charges she murdered her husband by poisoning him. The police will seize and examine the suspect's computer to uncover incriminating evidence such as the suspect's history of visiting web pages that deal with poisons. Once retrieved, the prosecutor will likely introduce that evidence to gain a conviction.

Digital evidence is not trivial. If it leads to a conviction on criminal charges, the defendant may face prison time. In a civil case, it can lead to a defendant having to pay monetary damages. And the police officers, technicians and private contractors who testify in court about digital evidence can be the difference between justice served and justice denied.

The "Wild West" of digital forensics

In some ways, the digital forensics landscape resembles the "Wild West." At least part of the reason for this is that digital forensics is not science-driven; instead, it is driven by its practitioners.

Those involved with determining the relevance of digital evidence are sometimes ill-equipped to make such assessments.

Problems, including inadequate training, use of outdated equipment, limited resources, few personnel and lack of a standardized protocol for analyzing digital evidence have all been documented. These shortcomings have led to evidentiary issues, improper conclusions by juries about digital evidence and doubtful outcomes. A good example would be the Casey Anthony trial, where improper analysis of her visits to websites dealing with murder was admitted as evidence.

Unlike DNA analysis, there's no standardized protocol for identifying, recovering, or processing digital evidence. As a result, two different technicians at different crime labs might reach different conclusions about a particular piece of evidence because they used different equipment or had divergent training.

These problems have implications for justice being served.

First steps toward standards

Thankfully, the situation is changing as the National Institute of Standards and Technology (NIST) works to develop specific standards for analyzing digital evidence.

The courts have also begun paying attention to some of the legal issues

involving digital evidence. For example, in Riley v California, the US Supreme Court ruled in 2014 that police must obtain a search warrant before they can seize electronic devices suspected of containing digital evidence. This ruling makes it somewhat harder for police to seize and analyze personal devices involved in crimes.

Lack of a code of ethics for practitioners

Because the people who recover, analyze, process and testify about digital evidence are influential in court proceedings, they must be ethical in their dealings with the legal system.

However, the reality is this: not only is digital forensics the "Wild West" when it comes to protocols for processing evidence, there isn't a code of ethics that governs the professional behavior of digital forensics practitioners.

Instead, various professional associations have created a hodgepodge of codes of ethics for members. Some of them are very detailed; others, not so much.

Unlike medicine or law, each of which has a single, overarching code of professional ethics enforced by the states, there is no comparable code that describes how a digital forensics practitioner should (or must) behave in his or her professional life.

The challenge of creating a code of ethics

Last May, I co-organized a two-day workshop on professional ethics and digital forensics that was funded by, and held at, the National Science Foundation (NSF). Academics, researchers and practitioners attended.

The workshop explored the need for a code of ethics and the contours of what such a code might include. We also examined hurdles to establishing a code, and existing codes from other professions that could serve as models.

The consensus among participants was that the need is great for a code of professional ethics that governs digital forensics practitioners. Participants shared examples of ethical issues that cloud the profession. Conflicts of interest. Vendors producing research on their own products and using that to influence agencies to adopt their product(s). Some practitioners' lack of understanding of the mechanics of the software they use to process evidence (the "black box" problem).

However, just because participants agree a code of ethics is needed doesn't mean there aren't significant hurdles to overcome with creating one. What specific behavior would be covered? What themes would the code address (for instance, "fairness," "trust," "justice")? What agency or organization would enforce the code? (Suggestions included NIST or the American Academy of Forensic Sciences (AAFS).) To whom would the code apply? All practitioners involved with digital evidence or just those processing it?

Moving forward

To raise awareness and continue working to create a code of ethics, this academic year we plan to replicate the workshop at various professional meetings including those of the Southern Criminal Justice Association, AAFS and the Academy of Criminal Justice Sciences.

We will also reach out to leaders in the AAFS and the American Bar Association for help with developing the code.

As digital evidence becomes more common in legal proceedings,

ensuring that practitioners have the strongest professional ethics is not only sensible, it is imperative.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation