Preface

In 2016, Apple and the FBI narrowly avoided litigation because hackers, of all folks, stepped in to provide the federal government with access to an iPhone that Apple said it did not have software to unlock. A former wrestling star obtained a landmark verdict against an online media outlet for streaming a sex video, and a former NFL star was litigating the admissibility of cell phone records, this time in a second murder trial. Issues of access to and the forensic use of electronic evidence are front and center to our social agenda.

Nowhere are those issues more complicated than in family law. Who but a spouse knows your passwords and might share legal title to the accounts that control your family’s information? For decades, family law attorneys have delved into family secrets, and dug for the information that one spouse has attempted to zealously guard from the other. Today, however, much of the sleuthing is electronic, and it requires an understanding of the technology that has woven its way into every aspect of our lives, and indeed expands in its use nearly every day.

As fresh and exciting as this legal work can be, one problem has remained constant during my long years of work in the field. In 1986, I was sitting in on an interview for a computer professional to take over the system at Rhode Island’s Department of the Attorney General. We were the National Crime Information Center (NCIC) criminal data repository for the state, so in addition to the usual issues attendant to supporting computers for 60 or so lawyers, investigators, and their staff, we had to maintain and manage a 24-hour-a-day interface to the national criminal
information system and host the database of Rhode Island’s criminal history information. All of Rhode Island’s law enforcement officers requesting criminal information from outside the state went through our systems, and all queries to the state from law enforcement within and without Rhode Island for this state’s criminal history data relied on our systems.

One job candidate touted his ability to “download application and systems requirement specifications” from “end-users,” and after he left, I explained to the Deputy AG who was in charge of the hire and who sat in on the interview that the candidate meant he felt that he could get folks at our office to communicate what they wanted the computers to do for them. The Deputy AG quipped that perhaps if the guy spoke English and thought of us as colleagues as opposed to “end-users,” we might find communication easier. Needless to say, someone who was a little less prone to geek-speak got the job.

At the time, a 355 megabyte drive cost around $32,000 and was about the size of a washing machine. A lot has changed in 30 years, but one truth remains the same—techno-babble does not facilitate communication when the fields of computers and law meet.

With that in mind, Aaron and I have done what we could to take some arcane and technical material, and to put it in terms that we hope will make sense to any lawyer, given that we lawyers have to communicate on the one hand with experts who have vast knowledge in the field, and on the other with judges who may have little familiarity beyond that required to send and read e-mail.

One great thing about our profession, however, is that it gives us the opportunity to delve into such diverse fields as accounting, psychology, and medicine, so computer forensics is just a more recent example of the many fields of expertise to become relevant to our work and attention. Hopefully, this guide will allow attorneys to strip away confusion, and to tackle the challenges that inevitably are becoming more and more common as electronic evidence becomes increasingly relevant in family law.

—Tim Conlon