Originally published on the *Legal Executive Institute* blog.
(www.legalexecutiveinstitute.com)

Reprinted with permission.

LEGAL EXECUTIVE INSTITUTE

The Neutral Corner: Using Forensic Neutrals in Trade Secret Disputes

Daniel Garrie May 2, 2017

Topics: Client Relations, Law Firm Profitability, Law Firms, Leadership, Legal Managed Services, Midsize Law Firms Blog Posts

The dirty secret of trade secret disputes is that even if you win, it can be difficult to get back to where you started. It's like closing the stable door after the horses have run off with trade secret disputes. A court or arbitration panel may not have trouble reaching findings of fact and conclusions of law, but the secrets are still out there. And ensuring that the trade secret information is entirely removed from the offending company's systems is a lot harder than rounding up wild horses.

Enter the forensic neutral. Forensic neutrals can help sort out the technical messes that often accompany trade secret disputes by:

- Helping to draft compliance with forensic protocols;
- Ensuring adherence to said protocols;

- Determining the existence and veracity of digital evidence;
- Forensically analyzing deleted or corrupted data for evidence of wrongdoing;
- Helping to obtain injunctive or preliminary relief, including "*ex parte* seizure" orders under the 2016 Defend Trade Secrets Act of 2016 (DTSA);
- Performing settlement-related or court-ordered purging of data from systems;
- Validating the removal of data from systems; *and*
- Auditing systems to ensure compliance with a court order or regulatory mandate.

The DTSA provides for a variety of situations in which a forensic neutral can be valuable. It states that an "owner of a trade secret that is misappropriated may bring a civil action under this subsection if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce."

As remedies, parties can seek damages and/or injunctive relief and, in certain situations, the DTSA allows for "*ex parte* seizure" of property if "necessary to prevent the propagation or dissemination of the trade secret." Because *ex parte* seizure applications are brought by the plaintiff without any notice to the defendant, and thus subject to potential abuse by an unscrupulous plaintiff, the DTSA sets out an extremely high standard that the plaintiff must meet, via sworn affidavit or verified complaint, to obtain an *ex parte* order. Forensic neutrals can be especially useful when "*ex parte* seizure" or other types of preliminary, injunctive relief is sought, as these types of relief often require the highly technical identification, collection, transfer and deletion of trade secret data.

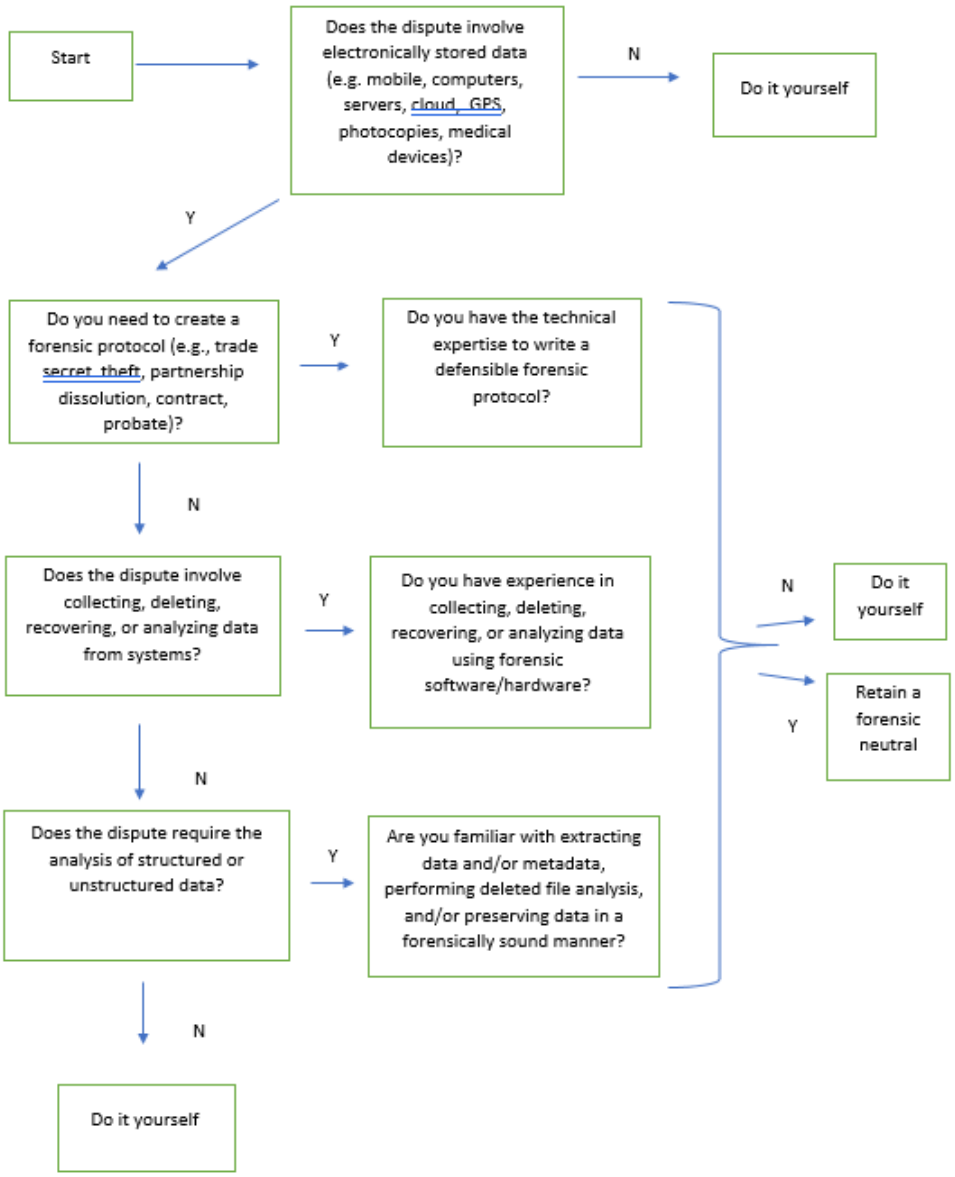
Making Sure Your Secrets are Deleted

Or consider another common trade secret scenario where employees go to work for a direct competitor of their former company, bringing with them gigabytes worth of confidential data. In response, the former employer seeks to enforce a confidentiality agreement that requires employees leaving the company to turn over all company data on their devices and accounts. The company invokes the arbitration clause in the employment agreement, and the arbitrator is prepared to rule in favor the company. Yet, the question remains: how can the arbitrator ensure an adequate remedy for the company? While it may be simple in theory to order the employees and their new employer to return the data and delete it from their systems, effectuating such an order, and ensuring actual, complete and continuing compliance, can be complicated.

One solution is to utilize a forensic neutral to help prepare a protocol for the identification and deletion of all the company's data in the possession of the employees and ensure compliance with the protocol. The exact scope of the forensic neutral's work can vary depending on the needs of the case, but the goal is to ensure the demands of the order are met from both a technical and legal perspective.

Forensic neutrals combine experience and training on both the technical and legal issues in these matters. As attorneys, forensic neutrals can help parties understand the technical requirements set forth by a protective order, draft necessary protocols and monitor compliance with a court order. As technologists, they can also perform the technical work themselves. This can save significant time and money, can often lead to quicker and more effective dispute resolutions, and can reassure the injured party that its trade secrets have been fully purged and protected.

While forensic neutrals can add value in many situations, not every case calls for one. Forensic neutrals are most useful in situations involving large volumes or highly sensitive electronically stored data; forensic protocols; collecting and analyzing data; purging data from computer systems; and/or performing deleted file analysis. The following flow chart can help in determining if a forensic neutral is appropriate:



By: Daniel Garrie
Senior Partner & Co-Founder
Law and Forensics

Daniel Garrie is the Senior Partner & Co-Founder for Law & Forensics, a consulting firm that specializes in e-discovery, software, computer forensics, and cybersecurity. Garrie leads a team that works with clients across industries on software, cybersecurity, e-discovery, and digital forensic issues all over the globe.

As a Neutral with JAMS, Garrie serves as an E-Discovery Special Master, Forensic Neutral, and Arbitrator with a focus on complex software and business litigation, privacy and data breach matters, trade secret theft, copyright and patent litigation disputes.

He is a nationally recognized educator and lecturer on various topics including computer software, cybersecurity, e-discovery, forensics, emerging Internet and mobile technologies, and cyberwarfare. He is the editor in chief of the Journal of Law & Cyber Warfare, a fellow at the Ponemon Information Privacy Institute, and on the Board of Advisors of several cybersecurity and technology start-ups.

Garrie is renowned as a Neutral for his ability to resolve e-discovery and related electronic matters involving companies and governmental entities. He is also frequently considered and appointed as Special Master by order of the court. Garrie's legal and computer science education and experience provide a unique perspective and an unsurpassed level of understanding needed to resolve legal/technology disputes.

Garrie also is a Cybersecurity Partner at Zeichner Ellman & Krause LLP.