Digital Discovery and Evidence Resources and Overview

Howard A. Kurtz

Kurtz & Blum P.L.L.C.
16 W. Martin St.; 10th Floor
Raleigh, NC 27601
(919) 832-7700
h.kurtz@kurtzandblum.com
http://www.kurtzandblum.com/tech-savvy-lawyers

Table of Contents

Introduction 3
Digital Evidence is Everywhere 4
Audio & Video 4
Audio and Video File Formats 5
Images 6
Documents 7
Computer Forensics 8
Metadata 9
Cellular Phones 10
Vehicle "Black Boxes" 11
Discovery from Social Networking Sites 11
Evidence with an Invisible Expiration Date 12
Conclusion 12
Useful Links 13
Appendix A 14
Federal Statute Limiting Social Network Sites' Ability to Disclose Subscriber Communications
Appendix B 16
Language of Request for Full Facebook Subscriber Information
Appendix C 18
Language for Inclusion in Letter to Prevent Spoliation of Digital Evidence
Appendix D 19
Language for Inclusion in Discovery Motions to Target Digital Evidence
Appendix E 20
North Carolina State Bar Ethics Opinion Regarding Metadata
Appendix F 25
N.C.G.S. §15A-211- Electronic Recording of Interrogations in Homicide Investigations
Appendix G 27
DOJ Collection of Digital Evidence Flow Chart

Introduction

Digital discovery and evidence are becoming ubiquitous elements in criminal defense work. Increasingly, defense attorneys must master many different forms of digital information in order to effectively understand and present their cases. Moreover, with the enactment of broad discovery provisions by the North Carolina legislature in 2005, a great deal of information that might previously have been merely arguably discoverable, or not really discoverable at all, now squarely falls within the all encompassing language of N.C.G.S. 15A-903. Combined with the technological advances in digital storage and the contemporaneous drop in the cost of data storage media, defense attorneys are rapidly finding themselves on the receiving end of a data deluge. In order to effectively represent our clients we must be able to rapidly cull valuable data from bulk data dumps. The digital wheat must be separated from the chaff. After it is secured and identified, that data must then be simplified and homogenized so it is understandable and so that its presentation is easy and clear.

Beyond the standard discovery that we have been given for quite some time, much of which is provided in a variety of audio or video formats in addition to the standard written documents and reports, we now receive a vast array of digital fingerprints and wakes allegedly left by our clients. These new types of evidence each require their own unique understanding as to how they are produced, maintained and how they are significant. Each new type of digital evidence has its own limitations and each has presents its own challenges. Many new types of digital evidence require defense attorneys to possess a new and discrete set of knowledge that is different from and in addition to that which we used to need to know.

At a time when the National Academy of Science has recognized tremendous flaws with the most basic and longest accepted of our forensic sciences, we now seem to be leaping headlong to embrace the newest of the forensic fields, that of digital forensics. Unfortunately, many defense attorneys seem to be willing to blindly accept this new field of forensics as a digital version of the gospel. Digital forensics seems to be accepted without question, with a level of trust and passivity that is belied by the lack of standards upon which this new “science” is based. Defense attorneys must quickly take the opportunity to learn the shortcomings of digital forensics and how they as advocates might grapple with such evidence when leveraged against their clients in plea negotiations or admitted against them in trial.

While digital forensics can prove as valuable as they can be misleading, digital techniques for organizing, accessing and analyzing discovery as well as presenting our cases can prove absolutely invaluable. In addition to information that we receive in digital format, much information that we receive in analog format can be digitized to increase the speed with which we can access it and exponentially increase the value that we can wring from it. Documents can and should be scanned; audio and video should be converted to standard workable formats. Once in fully digital form, the file can be easily transported, manipulated and mastered.

Below I have attempted to set out some of the types of data we can expect to receive or request and how to best deal with it once we have it. I have also included information on the types of experts that might be valuable in extracting or interpreting the data as well as programs that may help you present it to a prosecutor or in trial. Finally, following this outline are several excerpts from motions and requests, along with statutes and other miscellaneous resources that may prove helpful when crafting your own discovery motions or contemplating the use of digital evidence. I have also included a basic glossary for the uninitiated.

If anyone has questions about this material or would like to discuss how to best address issues surrounding the securing of or use of digital material, I would be happy to try and help. I can be reached at the number above.

Digital Evidence is Everywhere

All of our everyday lives are now documented in uncanny detail. All of our transactions are recorded on time and date stamped receipts that are saved on store servers. Gas stations, grocery stores and mega-marts have thorough high resolution security cameras posted in stores and in parking lots. ATMs take photos with every transaction. Cell phones can be used to at least roughly determine location. We communicate almost all the time and much of that information remains retrievable for substantial periods of time. Our computer searches can be tracked and even our cars can record our locations. Virtually everywhere we go and everything we do is digitally recorded.

This abundance of information can both help and hurt our clients. It can bolster or destroy an alibi or even provide insight as to someone's actual intent. If we fail to recognize the variety of sources from whence it can be retrieved, we will lose valuable evidence. Similarly if we fail to understand the limitations and volatility of digital evidence we might never know how to attack it. We must know how to find it and how to understand it. Perhaps most importantly we must learn to convey our comprehension so that others can understand it as well.

To some extent, we also need to ensure our clients understand the ramifications of life with an overabundance of digital communications. Just as we have always warned clients of speaking about their cases, we now must ensure they learn to keep their digital mouths shut as well. Texting about exploits or posting photos on My Space in which they are holding guns or drugs is simply a bad idea. We can also make sure to ask about whether such things might exist when speaking with new clients. It is best to know what you are dealing with at an early stage.

Audio & Video

Audio files are now frequently received in discovery. Their contents range from voicemails and recorded telephone calls to recorded audio from police interviews, wires or interrogations. Some departments now have audio recordings made from the feeds from the individual radios

that their officers wear at all times; consequently, if you deal with such a department in your jurisdiction, you should routinely request all such recordings.

Video files are now commonly received in discovery as well, whether from interrogations, undercover operations or surveillance video. Police cruisers are now often equipped with video cameras. Moreover, the recent requirements that police record all interrogations in homicide investigations has ensured that law enforcement is technologically prepared to record footage. There is much more video than there used to be and nothing easier for a jury to comprehend than a good video; everybody loves movies.

As with all discovery, a triage procedure is necessary. When significant numbers and / or duration of substantive audios are received, either separately or as part of a video, and you are preparing the case for trial, it is best to have them transcribed. Similarly, it is best not to simply rely on the transcription that you may be provided by law enforcement. Sometimes, they have a way of omitting things that may be of help to your client; other times they simply can't understand what our clients are saying.

Audio and Video File Formats

There are a multitude of digital audio and video file formats in use today and this is the source of untold problems. If you haven't yet, you should prepare to spend hours trying to figure out how to work with different types of audio or video files. The problem is that as techniques in digital compression have advanced, hardware manufacturers each chose their own formats. Some chose proprietary formats, requiring the purchase of their decoding software or "codec" and others used public domain formats. There are a tremendous number of formats and there are no players of which I am aware that play each and every one of them. As a result, to some extent, all of our experiences will require trial and error.

You will need software that has a variety of capabilities. Not all software can perform all functions, even with standard file types. Basic requirements include the ability to:

- Play a file normally
- Play a file starting at some particular spot
- Play a file with clear audio at faster than normal speed
- Allow cropping of segments to isolate small clips

More advanced skills will include the ability to:

- Transcode or convert the file to a standard audio or video format
- Lighten or darken a video
- Reduce background noise to make audio easier to understand
- Add subtitles to video

There are many different programs out there and I am not looking to drum up business for any particular company. But it is extremely helpful to find reliable software with which you are comfortable working. I have found that in working with audio and video that VLC Media Player is an excellent free program that can be downloaded off the web. Part of the advantage of using VLC, aside for its being free, is that it has all the codecs required to play most standard audio formats. One shortcoming is that VLC cannot work with .vob files, the format in which DVDs are recorded. A good player for .vob files is the GOM Media Player, which is also free.

VLC also has the ability to transcode, or convert, from and to a variety of formats. It is extremely cumbersome to need several different software tools to access audio or video in trial. The better practice is to convert all video (when possible) to one format, such as .avi, which is amenable to subtitles and to convert all audio (when possible) to one format, such as .mp3. Once in standard formats, you will only need standard tools to work with them.

Perhaps the single most valuable feature of VLC is its ability to speed up both audio and video. Reviewing files in faster than real time has tremendous and obvious advantages.

It is also worth noting that another free program, Audacity, provides extremely powerful tools for enhancing audio files. One caveat though, this particular software requires a significant degree of computer skill of its operator.

Sometimes you will run into a particular format that is not accessible through VLC or through whatever program you use. In those situations, simply Googling that file extension and downloading trial software or freeware (free software) is likely the best way to go.

Surely, not everyone is going to have the computer skills to manipulate digital files in an advanced fashion but everyone will need to develop basic skills. For those times that you can't manage those advanced editing tasks, it is time to look around the office for the biggest geek that you can find. Short of that, prepare to start asking for funding of experts.

A well edited audio or video clip is the most powerful tool that you can wield in either negotiating with a prosecutor or arguing to a jury. By well edited I simply mean that you have cut it to the shortest duration possible with crystal clear audio or subtitles so that they can't help but understand. A 15 minute video might be of value but if you can boil it down to 15 seconds you are more likely not to exceed your audience's attention span. It is better to work longer and harder getting it into a good usable clip than to try and fumble to advance a video to the right spot when all eyes are suddenly focused on you.

Images

Photos have always been commonplace items of evidence but now that everyone has a camera on their cell phone and now that the police are seizing computers that are occasionally full of photos, we need a better way to deal with them. Unlike the format issues that exist with audio

and video, most software will effectively access most photos. However, advantage can still be gained by using the right tools.

Picasa is a free download from Google that will automatically search a given directory for images. Once told to search it will load all photos into a single thumbnail gallery, allowing you to look at a great number of photos very quickly. It will even allow minor adjustments to lighting, etc.[1]

For serious image manipulation, The Gimp is an amazing free program. Can't imagine why you might need to seriously alter an image? If the State is intent on introducing a non-testifying co-defendant's written confession in which he implicates your client, how do you feel about their using a version in which they white out all the references to your client by name? Get the feeling that the jury will simply fill in the blanks?

So did the Supreme Court in Gray v. Maryland. 523 U.S. 185 (1998). In *Gray* they held that the redaction of a confession pursuant to *Bruton* should go beyond merely whiting out. Bruton v. United States, 391 U. S. 123 (1968). *Gray* opens wide the doors to image manipulation. Properly used, The Gimp can be used to alter a handwritten document, manipulated as an image, so that it appears to be entirely original and contains no reference to your client.

Documents

Documents are now frequently provided in Adobe .pdf format. These are simply scans that have been made of paper documents. If not provided in digital format, they can be scanned by you and saved as Adobe documents. Once in Adobe, large files are made highly portable and, when OCRed, easily searched.

OCR stands for Optical Character Recognition. It allows the computer to see a scanned document as text as opposed to as an image. It is very effective at decoding typed text though almost useless with handwritten material. Depending on the version of Adobe Acrobat you have, you may or may not have OCR capability. Though it is not free, the capability to OCR your discovery is amazingly useful.

Once OCRed, discovery can be assembled into an Adobe index. Indexed and OCRed discovery can be searched with lightning speed. Literally thousands of pages of OCRed and indexed can be searched using Boolean logic, the same type of search that you would use to do legal research on the computer. In a moment you can have a link to every reference to "Shooter" or "Tiny" that exists anywhere in the scanned discovery, so long as it is typed correctly.

[1] It should be noted that whenever making any type of audio or video adjustment that you should explain to the Court why you modified it and how it does not change the substance. Shown with an unmodified original you should be able to explain why the augmented version is preferable. The State has used techniques like enhanced video for quite some time so this should not present a problem.

There is no substitute for OCRed discovery in a case where you have a volume of information. It enables instant access to information that used to require hours of inserting physical tabs and creating indices.

If your resources exceed my recollection of the resources available as a public defender, the addition of Casemap to OCRed discovery is a good one. Casemap allows you to highlight individual facts in the discovery and hyperlink directly to that information. It is a relational database that is easy to use but powerful. Once you have put your discovery into Casemap, not an easy task to be sure, you will be able to access data by person, place, time or event. It makes for effective dissection of issues and easy prep for witnesses examinations. However, the cost of admission is both monetary and temporal. Mapping discovery into Casemap requires a tremendous amount of time in order for it be worthwhile.

Computer Forensics

Computer forensics is a broader and more complicated topic than can easily be summarized in this paper. In simple terms, it is simply a scientific examination of the data on digital storage media. The material examined could be in the form of a laptop, desktop, hard drive, server, memory card, jump drive, CD or DVD.

The first step for law enforcement in a case involving computer forensics is for them to procure a search warrant for the data within the seized item. Though the courts have been lax in enforcing the requirements, the warrant should limit the scope of the search so that law enforcement does not simply wade through all of a person's private data and communications. The scope of the search is transmitted to the examiner performing the search.

Most law enforcement uses either EnCase or Forensic Tool Kit (FTK) to perform their examinations. Both those software packages produce standard results that are theoretically limited by the scope terms they are provided (such as "meet me", "underage photos", etc.). In reality, I am unsure how much the scope of their search actually limits the scope of their search.

Once they have a warrant, the search performed should be according to forensically acceptable guidelines (see Appendix G, U.S. Department of Justice Examination of Digital Evidence Flow Chart). A proper exam requires that a perfect copy of the material to be examined be made. That copy is produced by using a write blocking mechanism so that the data can't be modified during the search. As the copy is made, a cryptographic hash is created (commonly an MD5 hash). The cryptographic hash is a series of numeric values that can be matched with future copies of the same data. If nothing has been changed, that value should match from copy to copy.

There are situations when a "live" or "preview" search is performed on a system. From a forensic perspective, such a search is problematic as it allows data to be modified subsequent

to the device coming into law enforcement custody but before it is assigned a cryptographic hash.

Forensic examinations can produce a tremendous amount of information. Computers store search history, internet browsing history, and a variety of forms of communications along with the metadata associated with them. Moreover, law enforcement may find sufficient information from which they can apply to the court for orders to produce records of email providers or social network hosts.

The results produced from a forensic examination will contain both current items and items that were deleted. Using email as the example, unless specifically deleted, sent emails are retained forever. Specifically deleted emails are stored in the deleted items folder until it is manually emptied. After the deleted email folder is emptied, those deleted deleted emails are still likely retrievable. It may well be that at some point the computer would happen to use that same space on the hard drive to store new information, but until it does, that deleted deleted information will likely remain on the hard drive in a fashion that can be retrieved.
The information found on a computer does not necessarily come from a particular person, however. Most computers are now on wireless connections that are extremely vulnerable to hacking. Though traditionally thought of as requiring skill, hacking today simply requires the will to do it. The web is full of free software that empowers anyone who wishes to hack into wireless and or computers.

As a result of the permeability of computer security, the desire for anonymity and a desire to defeat computer forensics, the field of antiforensics has emerged. Antiforensics is geared to defeating the value of computer forensics or facilitating the planting of fake information to mislead forensic examiners. As one example, the Metasploit Project is an organization dedicated to the creation of just such software. One of their programs, Timestomp, exists solely so that people can alter the metadata associated with a file.

Lawyers should note that communications with clients are of a sensitive nature, email is to be avoided. If a computer containing such emails is eventually seized, the ensuing argument over privilege is one to be avoided as it is extremely time consuming to go through a hard drive with an eye toward noting all potentially privileged communications. The best practice is not to email any privileged information to clients.

Metadata

The easiest way to think of Metadata is simply that it is data about data (per Wikipedia). This may be an oversimplification but is still a valuable way to conceive of it.

For a document the information contained in metadata may include: how long the document is, who the author is, when the document was written, and a short summary of the document. For a photo the information contained in metadata typically includes: how large a picture is, the

color depth, the image resolution, when an image was created, type of camera, quality of image, and the date the image was last modified. Other types of metadata include the IP address from which email is sent and the date and time temporary internet files are created.

The admissibility of metadata has been the subject of some debate. Initially the courts were loathe to admit it as evidence but the trend is to allow electronically generated evidence, metadata, to be admitted. However, questions remain as to how that data is validated. The question of validation includes things as simple as whether the clock was set correctly and can range to whether the hardware or software were working properly at the time the information was recorded. Though this may be considered by courts to go more to weight than admissibility, the question of whether this is valid evidence is one that should be posed. Some see metadata as tantamount to computer generated hearsay, despite what seems to be an emerging view to the contrary.

As lawyers, we now have some State Bar guidance on the subject of metadata (see Appendix E). The main thrust is that we must 1. Be careful not to divulge client information through unintentional transmission of metadata; and 2. Refrain from viewing metadata that may have been unintentionally transmitted to us by opposing counsel. It is always prudent to use a mechanism by which to delete all metadata before sending out a document.

However, when it comes to discovery, we are entitled by statute to the *complete* files of law enforcement. We should thus be arguing for the State to be required to provide all files from law enforcement in native format, that is, the original format in which it was created. If received in native format, we are then able to view the metadata such as when and by whom a document was created. Nothing in the Bar opinion would prevent seeking or reviewing said data.

Cellular Phones

Cellular phones are now essentially small computers. The amount of information that one is capable of containing is staggering. They can contain text messages, emails, Facebook information, voicemails, chat logs, photos and videos just as computers do. Forensics of cell phones is practically indistinguishable from that of computers with the exception of triangulation. The location of a cell phone when a call is made or received can be approximated by reference to the cellular tower that the phone used to connect to the cellular provider. Furthermore, it specifies the 120 degree arc in which the phone is located by noting the side of the tower hit. This type of evidence is less than precise as it is affected by landscape, weather conditions, tower strength among other things. Newer cell phones may have GPS enabled, though, which can yield location with great precision.

Vehicle "Black Boxes"

Some cars now have so-called "black boxes", similar to those that are on aircraft. In cases involving accidents, the data downloaded from these mini-computers generally contains the speed on impact, whether the car was accelerating or decelerating at impact, whether the brakes were applied and whether a car stopped at the scene.

Discovery from Social Networking Sites

People now record a tremendous amount of information on social networking sites like Facebook or My Space. People store photos and conversations. It is remarkable how much private information people will store on their site. Some of that information can be incredibly inculpatory, like photos of your client wearing a victim's clothing. Other information can be valuable to a defense, like an alleged victim expressing violent intent toward your client. For obvious reasons, there is much potential evidence on these sites.

However, chapter 18 of the United States Code, section 2702, seems to enable law enforcement to secure text messaging and other forms of communications from social networking sites. There is no provision whatsoever for defense attorneys, or even the courts, unless they are operating on behalf of law enforcement, to obtain said information.

According to Facebook, they will recognize only law enforcement subpoenas or court orders on behalf of law enforcement. While the constitutionality of depriving defense counsel of potentially exculpatory evidence seems dubious, as a practical matter, the might of Facebook's corporate counsel's ability to effectively prevent the securing of said information is likely quite real. I have not included the actual text of their subpoena requirements as they emphasize that the material is not to be disseminated to anyone who is not law enforcement and we are decidedly not law enforcement. Instead, a website containing that information can be found at http://dtto.net/docs/facebook-manual.pdf. To contact Facebook directly, they can be emailed at subpoena@facebook.com. The scope of information that people put on Facebook is incredible and so the value of retrieving such information should not be underestimated. It may require substantial legal wrangling, however.

In response to a *Ritchie* styled *ex parte* motion, I have been successful in obtaining some Facebook information. Though the motion itself is beyond the scope of this manuscript, I have included the specifics of that request listing the information we sought, in accordance with Facebook's policies. If someone has additional specific questions about this motion, I would be happy to discuss it with them privately. That document is included herein as appendix

It is worthy of note to mention that impersonation of another Facebook member is a violation of Facebook rules and may be interpreted as a violation of the NC Rules of Professional Conduct. It is the subject of a Philadelphia Bar Association non-binding advisory opinion, 2009-02, in which it was held to be unethical.

Evidence with an Invisible Expiration Date

While it is true that the evidence contained an actual hard drive or cell phone should be stable and is hopefully carefully preserved by law enforcement, those items almost certainly contain merely a fraction of currently available relevant information. Though some information from social networking and web based email accounts may be located on a forensic image of the seized computers, that information represents a small portion of the relevant and potentially exculpatory information that is discoverable. Each site maintains its own servers upon which client data is stored. That means that each and every photo or message ever sent from an account is maintained on the server even after the person might have deleted it off of their visible page or deleted the email from their inbox of their personal computer. It means that there is likely much more data available at the server, the source, than there would ever be on an individual computer.

The source servers retain data for some period of time after it is last accessed and some period of time after an account is either idle or deactivated. However, sites generally guard their data retention policy and some seem to consider it an industry secret. Thus, it is unknown whether individual datum is deleted daily after a certain period of time or if all data is deleted as a whole after some period of time. This invisible expiration date makes this request extremely time sensitive.

Conclusion

Whether computers and digital evidence are of interest to you, or not, they are now a permanent part of the landscape. The ability to understand rudimentary computer forensics digital evidence is an absolute necessity. The ability to work with digital evidence skillfully will be a tremendous asset.

Useful Links

Computer Forensics:

Unites States Department of Justice- Forensics Web Page
www.ojp.usdoj.gov/nij/topics/forensics/welcome.htm

Unites States Department of Justice- Forensic Exam of Digital Evidence by Law Enforcement
www.ojp.usdoj.gov/nij/pubs-sum/199408.htm

Courtroom use of Digital Evidence

Unites States Department of Justice- Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors
www.ojp.usdoj.gov/nij/pubs-sum/211314.htm

Handout from Cheryl Howell's Presentation to North Carolina's District Court Judges on Electronic Evidence
www.sog.unc.edu/programs/dcjudges/2009SummerConference/HowellElectronicEvidenceHandout2.pdf

Law Enforcement Access to Electronic Communications

Jeff Welty- NC Institute of Government Administration of Justice Bulletin Prosecution and Law Enforcement Access to Information about Electronic Communications
http://www.sog.unc.edu/pubs/electronicversions/pdfs/aojb0905.pdf

Appendix A

Federal Statute Limiting Social Network Sites' Ability to Disclose Subscriber Communications

18 U.S.C. § 2702. Disclosure of Contents

(a) Prohibitions.--Except as provided in subsection (b)—

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) Exceptions.--A person or entity may divulge the contents of a communication–

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or

(6) to a law enforcement agency—

(A) if the contents—

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

(B) if required by section 227 of the Crime Control Act of 1990 [42 U.S.C.A. S13032].

(C) if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay.

(c) Exceptions for disclosure of customer records. A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))—

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information; or

(5) to any person other than a governmental entity.

Appendix B

Language of Request for Full Facebook Subscriber Information

Exhibit A

1. Provide any and all information pertaining to the account related to the following information:

   User ID: NUMBER
   Email: EMAIL ADDRESS
   Full name of user: NAME
   Networks: NETWORK
   Birth date: BIRTH DATE

   This information should be provided in a standard Microsoft word document format which can be viewed with non-proprietary software. The data should be in a format that does not need to be deciphered and can be understood in the format that it is provided in.

2. Provide any and all account activity from the date the above account was created through DATE. This information should be provided in a standard Microsoft word document format which can be viewed with non-proprietary software.

3. Provide any and all account activity from DATE through DATE for user ID NUMBER. This information should be provided in a standard Microsoft word document format which can be viewed with non-proprietary software.

4. Provide the Neoprint of user ID NUMBER. This information should be provided in a standard Microsoft word document format which can be viewed with non-proprietary software.

5. Provide Photoprint of user ID NUMBER. Photos should be provided in a standard image format which can be viewed with non-proprietary software.

6. Provide Contact information specified by user ID NUMBER. This information should be provided in a standard Microsoft word document format which can be viewed with non-proprietary software

7. Provide the text and any and all data related to personal messages sent, received, or viewed by user ID NUMBER. This information should be provided in a standard Microsoft word document format which can be viewed with non-proprietary software.

8. Provide the text and any and all data related to wall posts received by user ID NUMBER. This information should be provided in a standard Microsoft word document format which can be viewed with non-proprietary software.

9. Provide the text and any and all data related to wall posts sent by user ID NUMBER. This information should be provided in a standard Microsoft word document format which can be viewed with non-proprietary software.

10. Provide the IP log of user ID NUMBER. Please provide the whole date range. I understand when requesting the whole date range that the logs may not be complete. This information should be provided in a standard Microsoft word document format which can be viewed with non-proprietary software.

11. Provide any and all information that was deleted from user ID NUMBER after DATE. This information should be provided in a standard Microsoft word document format which can be viewed with non-proprietary software.

12. Provide a list of anyone who requested information for the above account. This includes but is not limited to requests for: data inquires, any requests to deactivate the account, any request to purge any information in the account. This information should be provided in a standard Microsoft word document format which can be viewed with non-proprietary software.

Appendix C

Language for Inclusion in Letter to Prevent Spoliation of Digital Evidence

This is a notice and demand that critical evidence in the above-referenced matter exists in the form of electronic data contained in computer systems, cellular phones and/or Palm, Treo, Blackberry or other PDA devise(s) used by NAME and/or NAME, including but not limited to any CPU, laptop, flash memory device, floppy disk, compact disc, hard drive, digital video disc, Subscriber Identity Module (SIM) cards or other electronic media be immediately preserved in its present state and that there be no spoliation or alteration of their data. This evidence must be immediately preserved and retained until further written notice of the undersigned. This request is essential, as a paper printout of text contained in computer files or SIM cards does not completely reflect all information contained within the electronic files. Additionally, the continued operation of the computer systems identified herein could likely result in the destruction of relevant evidence due to the fact that electronic evidence can be easily deleted, altered or otherwise modified. The failure to preserve and retain the electronic data outlined herein in this notice constitutes spoliation of evidence.

For the purposes of this notice, "Electronic Data" shall include but not be limited to all text files (including word processing documents), spreadsheets, e-mail files and information concerning e-mail (including but not limited to logs of e-mail history and usage, header information and deleted files), Internet history files and preferences, graphical image files, (including but not limited to JPG, GIF, BMP, TIFF and WAV files), databases, calendars and scheduling information, computer systems activity logs, text messages, voicemails, address books, and all file fragments and backup files containing Electronic Data. Please preserve and retain all Electronic Data generated or received by NAME and/or NAME.

Appendix D

Language for Inclusion in Discovery Motions to Target Digital Evidence

1. Duplicates of any forensic copies made by the State, prosecution's experts or any other prosecutorial agency of any computer hard drives or digital storage media including but not limited to CD-ROMS, USB flash drives, floppy disks, memory cards, digital camera storage, smart cards, router logs and portable hard drives.

2. Duplicates of any forensic copies made by the State, prosecution's experts or any other prosecutorial agency of any cell phone and or SIM cards, media cards or other storage used in conjunction with telephony.

3. Duplicates of any forensic copies made by the State, prosecution's experts or any other prosecutorial agency of any digital media retrieved from blogs, micro-blogs / twitter sites, social networking hosts, websites, web hosts, internet service providers or internet mail providers. Said request includes but is not limited to any SMS and RSS data as well as all related metadata.

4. In the event prosecution's experts did not make a forensic copy of any original media referenced herein, defense requests that forensically sound copies be made and furnished to the defense for examination by the defense expert.

5. A complete inventory of all items taken that may contain any type of digital data, whether or not such items were examined or copied by prosecution's experts.

6. A complete copy of all forensics reports, chain of custody records, and lab notes generated by prosecution's experts pertaining to the acquisition, preservation, analysis, and or reporting by said experts in the course of this investigation.

Appendix E

North Carolina State Bar Ethics Opinion Regarding Metadata

2009 Formal Ethics Opinion 1; January 15, 2010
Review and Use of Metadata

Opinion rules that a lawyer must use reasonable care to prevent the disclosure of confidential client information hidden in metadata when transmitting an electronic communication and a lawyer who receives an electronic communication from another party or another party's lawyer must refrain from searching for and using confidential information found in the metadata embedded in the document.

Background

In the representation of clients in all types of legal matters, lawyers routinely send emails and electronic documents, spreadsheets, and PowerPoint presentations to a lawyer for another party (or directly to the party if not represented by counsel). The email and the electronic documents contain metadata1 or embedded information about the document describing the document's history, tracking and management2 such as the date and time that the document was created, the computer on which the document was created, the last date and time that a document was saved, "redlined" changes identifying what was changed or deleted in the document, and comments included in the document during the editing process. Pennsylvania Bar Ass'n. Comm. on Legal Ethics and Professional Responsibility, Formal Opinion 2007-500, *reconsidered* Pennsylvania Formal Op. 2009-100, notes that, although most metadata contains "seemingly harmless information," it may also contain "privileged and/or confidential information, such as previously deleted text, notes, and tracked changes, which may provide information about, e.g., legal issues, legal theories, and other information that was not intended to be disclosed to opposing counsel." This embedded information may be readily revealed by a "right click" with a computer mouse, by clicking on a software icon, or by using software designed to discover and disclose the metadata.3 On occasion, one software application automatically displays or uses metadata that another software application hides from the user. The sender of the document may be unaware that there is metadata embedded in the document or mistakenly believe that the metadata was deleted from the document prior to transmission. The Ethics Committee is issuing this opinion sua sponte in light of the importance of the ethical issues raised by metadata.

Inquiry #1:

What is the ethical duty of a lawyer who sends an electronic communication to prevent the disclosure of a client's confidential information found in metadata?

Opinion #1:

Rule 1.6(a) of the Rules of Professional Conduct prohibits a lawyer from revealing information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized to carry out the representation, or disclosure is permitted by one of the exceptions to the duty of confidentiality set forth in paragraph (b) of the rule. As noted in comment [20] to the rule, "[w]hen transmitting a communication that includes information acquired during the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients." Therefore, a lawyer who sends an electronic communication must take reasonable precautions to prevent the disclosure of confidential information, including information in metadata, to unintended recipients.4

RPC 215 addressed the preservation of confidential client information when using modern forms of communication including cellular phones and email. The opinion states that the professional obligation to use reasonable care to protect and preserve confidential information extends to the use of communications technology; "[h]owever, this obligation does not require that a lawyer use only infallibly secure methods of communication." Nevertheless, "a lawyer must take steps to minimize the risks that confidential information may be disclosed in a communication."

Lawyers have several options to minimize the risk of disclosing confidential information in an electronic communication. Lawyers should exercise care in using software features that track changes, record notes, allow "fast saves," or save different versions, as these features increase the amount of metadata within a document. Metadata "scrubber" applications remove embedded information from an electronic document and may be used to remove metadata before sending an electronic document to opposing counsel. Finally, lawyers may opt to use an electronic document type that does not contain as much metadata, such as the portable document format (PDF), or may opt to use a hard copy or fax. Both commercial and freeware software solutions exist to help lawyers avoid inadvertently disclosing confidential information in an electronic communication.

What is reasonable depends upon the circumstances including, for example, the sensitivity of the confidential information that may be disclosed, the potential adverse consequences from disclosure, any special instructions or expectations of a client, and the steps that the lawyer takes to prevent the disclosure of metadata. Of course, when electronic communications are produced in response to a subpoena or a formal discovery request in civil litigation, the responding lawyer may not remove or restrict access to the metadata in the communications if doing so would violate any disclosure duties under law, the Rules of Civil Procedure, or court order.

Inquiry #2:

May a lawyer who receives an electronic communication from another party or the party's lawyer search for and use confidential information embedded in the metadata of the communication without the consent of the other party or lawyer?

Opinion #2:

No, a lawyer may not search for confidential information embedded in metadata of an electronic communication from another party or a lawyer for another party. By actively searching for such information, a lawyer interferes with the client-lawyer relationship of another lawyer and undermines the confidentiality that is the bedrock of the relationship. Rule 1.6. Additionally, if a lawyer unintentionally views confidential information within metadata, the lawyer must notify the sender and may not subsequently use the information revealed without the consent of the other lawyer or party.

The New York State Bar was the first to adopt the position that a lawyer should not search metadata for confidential information. The state bars of Alabama, Arizona, Florida, and Maine have followed this position.5 New York Ethics Opinion 749 holds that,
in light of the strong public policy in favor of preserving confidentiality as the foundation of the lawyer-client relationship, use of technology to surreptitiously obtain information that may be protected by the attorney-client privilege, the work product doctrine, or that may otherwise constitute a "secret" of another lawyer's client would violate the letter and spirit of [the New York] Disciplinary Rules.

Agreeing with the position of the New York State Bar, the Alabama State Bar Disciplinary Commission in Opinion 2007-02 finds that, "[t]he mining of metadata constitutes a knowing and deliberate attempt by the recipient attorney to acquire confidential and privileged information in order to obtain an unfair advantage against an opposing party." Although the ABA Standing Committee on Ethics and Professional Responsibility, in Formal Opinion 06-442 (2006),6 takes the position that the Model Rules of Professional Conduct do not prohibit a lawyer from reviewing and using metadata, this position was subsequently rejected by the State Bar of Arizona among others. Arizona Opinion 07-03 observes that under the ABA opinion, which puts "the sending lawyer…at the mercy of the recipient lawyer…, the sending lawyer might conclude that the only ethically safe course of action is to forego the use of electronic document transmission entirely…[this is not] realistic or necessary."

The North Carolina State Bar Ethics Committee agrees that a lawyer may not ethically search for confidential information embedded within an electronic communication from another party or the lawyer for another party. To do so would undermine the protection afforded to confidential information by Rule 1.6 and would interfere with the client-lawyer relationship of another lawyer in violation of Rule 8.4(d), which prohibits conduct that is "prejudicial to the administration of justice."

The Ethics Committee recognizes that it is possible for a lawyer to unintentionally find confidential information upon viewing the contents of an electronic communication. If this occurs, the lawyer must notify the sender and may not subsequently use the information revealed without the consent of the other lawyer or party.

Rule 4.4(b) requires a lawyer who receives a writing relating to the representation of a client that the lawyer knows, or reasonably should know, was inadvertently sent, to promptly notify the sender. Receiving confidential information embedded in the metadata of an electronic communication is analogous to receiving, for example, a faxed pleading that inadvertently includes a page of notes from opposing counsel. Although the receiving lawyer did not seek out the confidential information, the receiving lawyer in either situation has a duty to "promptly notify the sender" under Rule 4.4(b) if the receiving lawyer "knows or reasonably should know that the writing was inadvertently sent." Although the technology involved is different, the Ethics Committee believes that a lawyer who can recognize confidential information inadvertently included in a fax can also recognize confidential information inadvertently included in an electronic document.

Further, a lawyer who intentionally or unintentionally discovers confidential information embedded within the metadata of an electronic communication may not use the information revealed without the consent of the other lawyer or party.

Although the receipt of confidential information embedded in metadata is analogous to the receipt of a page of handwritten notes in a faxed pleading for purposes of notifying the sender under Rule 4.4(b), metadata differs from the readily apparent information contained in a paper communication. Confidential information may inadvertently be included in the metadata of an electronic document despite reasonable efforts by a sender to stay abreast of rapid technological changes and to prevent the transmission of confidential information. The exchange of electronic documents, however, is vital to the functioning of the legal profession in the twenty-first century. Although Rule 4.4(b) does not require a lawyer to return an inadvertently sent paper document or specifically prohibit the use of information contained in such a document, Rule 8.4(d) prohibits conduct that is "prejudicial to the administration of justice." As comment [4] to Rule 8.4 observes, "[t]he phrase 'conduct prejudicial to the administration of justice' in paragraph (d) should be read broadly to proscribe a wide variety of conduct, including conduct that occurs outside the scope of judicial proceedings." Allowing the use of confidential information that is found embedded within metadata would inhibit the efficient functioning of the modern justice system and also undermine the protections for client confidences in the Rules of Professional Conduct and the attorney-client privilege. Therefore, the use of found metadata is "prejudicial to the administration of justice" in violation of Rule 8.4(d) and is prohibited.

In summary, a lawyer may not search for and use confidential information embedded in the metadata of an electronic communication sent to him or her by another lawyer or party unless the lawyer is authorized to do so by law, rule, court order or procedure, or the consent of the

other lawyer or party. If a lawyer unintentionally views metadata, the lawyer must notify the sender and may not subsequently use the information revealed without the consent of the other lawyer or party.

Endnotes

1. Metadata is explained in Pennsylvania Bar Ass'n. Comm. on Legal Ethics and Professional Responsibility, Formal Op. 2007-500 (2007), *reconsidered* Pennsylvania Formal Op. 2009-100 (2009), as follows: "Metadata, which means 'information about data,' is data contained within electronic materials that is not ordinarily visible to those viewing the information. Although most commonly found in documents created in Microsoft Word, metadata is also present in a variety of other formats, including spreadsheets, PowerPoint presentations, and Corel WordPerfect documents."

2. Arizona State Bar Comm. on the Rules of Professional Conduct, Op. 07-03 (2007).

3. Pennsylvania Formal Op. 2007-500 (2007), *reconsidered* Pennsylvania Formal Op. 2009-100 (2009).

4. This is consensus position among the jurisdictions that have considered the issue as well as the ABA Standing Committee on Ethics and Professional Responsibility. Alabama State Bar Disciplinary Comm'n, Op. 2007-02 (2007); Arizona State Bar Comm. on the Rules of Professional Conduct, Op. 07-03 (2007); Colorado Bar Ass'n. Ethics Comm., Op. 119 (2008); District of Columbia Legal Ethics Comm., Op. 341 (2007); Florida Professional Ethics Comm., Ethics Op. 06-2 (2006); Maine Bd. of Bar Overseers Professional Ethics Comm'n., Op. 196 (2008); Maryland State Bar Ass'n. Comm. on Ethics, Op. 2007-09 (2006); New York State Ethics Op. 782 (2004); Pennsylvania Formal Op. 2009-100 (2009); ABA Standing Comm. on Ethics and Professional Responsibility, Formal Op. 06-442 (Aug. 5, 2006).

5. Alabama Ethics Op. 2007-02 (2007); Arizona Op. 07-03 (2007); Florida Ethics Op. 06-2 (2006); Maine Op. 196 (Oct. 21, 2008); and New York Ethics Op. 749 (2001). District of Columbia Legal Ethics Comm. Op. 341 (2007) holds that a lawyer may not view metadata if the lawyer has actual knowledge that it was provided inadvertently.

6. ABA Formal Op. 06-442 (2006) concludes that the Model Rules of Professional Conduct permit a lawyer to review and use metadata contained in email and other electronic documents. The Colorado Bar Association, Maryland State Bar Association, and Pennsylvania Bar Association agree with the position expressed in the ABA opinion. Colorado Op. 119 (2008); Maryland Op. 2007-09 (2006); Pennsylvania Op. 2009-100 (2009).

Appendix F

N.C.G.S. §15A-211- Electronic Recording of Interrogations in Homicide Investigations

§ 15A-211. Electronic recording of interrogations.

(a) Purpose. – The purpose of this Article is to require the creation of an electronic record of an entire custodial interrogation in order to eliminate disputes about interrogations, thereby improving prosecution of the guilty while affording protection to the innocent and increasing court efficiency.

(b) Application. – The provisions of this Article shall only apply to custodial interrogations in homicide investigations conducted at any place of detention.

(c) Definitions. – The following definitions apply in this Article:

(1) Electronic recording. – An audio recording that is an authentic, accurate, unaltered record; or a visual recording that is an authentic, accurate, unaltered record.

(2) In its entirety. – An uninterrupted record that begins with and includes a law enforcement officer's advice to the person in custody of that person's constitutional rights, ends when the interview has completely finished, and clearly shows both the interrogator and the person in custody throughout. If the record is a visual recording, the camera recording the custodial interrogation must be placed so that the camera films both the interrogator and the suspect. Brief periods of recess, upon request by the person in custody or the law enforcement officer, do not constitute an "interruption" of the record. The record will reflect the starting time of the recess and the resumption of the interrogation.

(3) Place of detention. – A jail, police or sheriff's station, correctional or detention facility, holding facility for prisoners, or other facility where persons are held in custody in connection with criminal charges.

(d) Electronic Recording of Interrogations Required. – Any law enforcement officer conducting a custodial interrogation in a homicide investigation shall make an electronic recording of the interrogation in its entirety.

(e) Admissibility of Electronic Recordings. – During the prosecution of any homicide, an oral, written, nonverbal, or sign language statement of a defendant made in the course of a custodial interrogation may be presented as evidence against the defendant if an electronic recording was made of the custodial interrogation in its entirety and the statement is otherwise admissible. If the court finds that the defendant was subjected to a custodial interrogation that was not electronically recorded in its entirety, any statements made by the defendant after that non-electronically recorded custodial interrogation, even if made during an interrogation that is otherwise in compliance with this section, may be questioned with regard to the voluntariness and reliability of the statement. The State may establish through clear and convincing evidence that the statement was both voluntary and reliable and that law enforcement officers had good cause for failing to electronically record the interrogation in its entirety. Good cause shall include, but not be limited to, the following:

(1) The accused refused to have the interrogation electronically recorded, and the refusal itself was electronically recorded.

(2) The failure to electronically record an interrogation in its entirety was the result of unforeseeable equipment failure, and obtaining replacement equipment was not feasible.

(f) Remedies for Compliance or Noncompliance. – All of the following remedies shall be granted as relief for compliance or noncompliance with the requirements of this section:

(1) Failure to comply with any of the requirements of this section shall be considered by the court in adjudicating motions to suppress a statement of the defendant made during or after a custodial interrogation.

(2) Failure to comply with any of the requirements of this section shall be admissible in support of claims that the defendant's statement was involuntary or is unreliable, provided the evidence is otherwise admissible.

(3) When evidence of compliance or noncompliance with the requirements of this section has been presented at trial, the jury shall be instructed that it may consider credible evidence of compliance or noncompliance to determine whether the defendant's statement was voluntary and reliable.

(g) Article Does Not Preclude Admission of Certain Statements. – Nothing in this Article precludes the admission of any of the following:

(1) A statement made by the accused in open court during trial, before a grand jury, or at a preliminary hearing.

(2) A spontaneous statement that is not made in response to a question.

(3) A statement made during arrest processing in response to a routine question.

(4) A statement made during a custodial interrogation that is conducted in another state by law enforcement officers of that state.

(5) A statement obtained by a federal law enforcement officer.

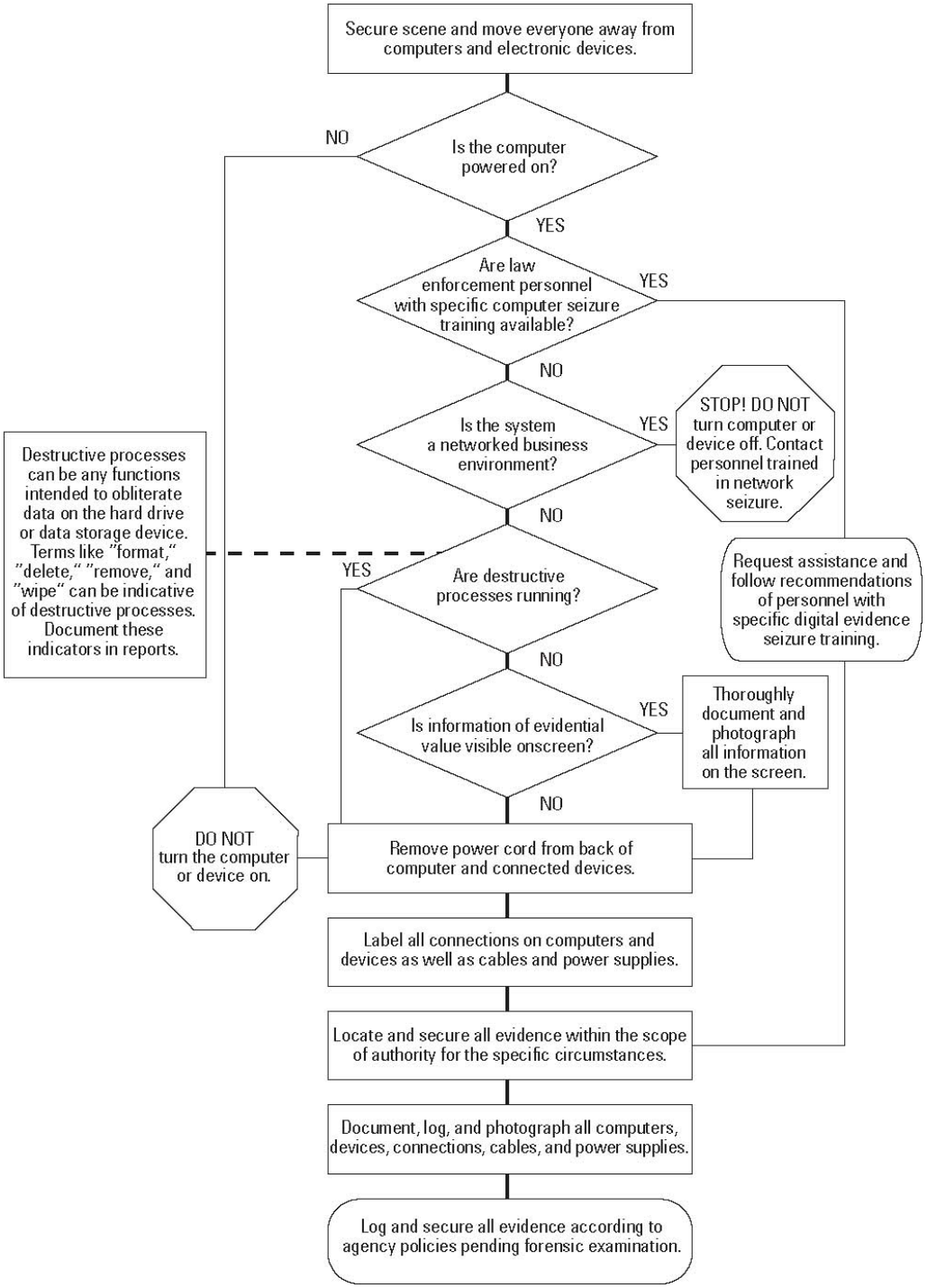
(6) A statement given at a time when the interrogators are unaware that the person is suspected of a homicide.

(7) A statement used only for impeachment purposes and not as substantive evidence.

(h) Destruction or Modification of Recording After Appeals Exhausted. – The State shall not destroy or alter any electronic recording of a custodial interrogation of a defendant convicted of any offense related to the interrogation until one year after the completion of all State and federal appeals of the conviction, including the exhaustion of any appeal of any motion for appropriate relief or habeas corpus proceedings. Every electronic recording should be clearly identified and catalogued by law enforcement personnel. (2007-434, s. 1.)

Appendix G

DOJ Collection of Digital Evidence Flow Chart



From the U.S. Department of Justice's Research and Development Branch, the National Institute of Justice