Cyber Evidence Resource Compilation

I. Crime Analysis and Mapping

***Analysis Toolkit*, BUREAU OF JUST. ASSISTANCE, U.S. DEP'T OF JUST. (2020), https://it.ojp.gov/AT/ (last visited Apr. 20, 2020).**
The Analysis Toolkit enables users to explore existing resources, refine current approaches, and discover new points of contact. The toolkit was developed with support of the DOJ's Bureau of Justice Assistance (BJA) as a clearinghouse for publicly available crime and intelligence analysis resources. With the support of the Institute for Intergovernmental Research, a group of subject experts in the fields of crime and intelligence analysis identified content for the toolkit and continue to evaluate the resources on the site to ensure relevancy. The toolkit contains several case studies resulting from the Nationwide Crime Analysis Capability Building Project, which was initiated by BJA to identify and evaluate promising practices to assist jurisdictions in enhancing their crime analysis capacity.

JOHN B. ECK ET AL., OFF. OF JUST. PROGRAMS, U.S. DEP'T OF JUST., MAPPING CRIME: UNDERSTANDING HOTSPOTS (2005), https://www.researchgate.net/publication/32894301_Mapping_Crime_Understanding_Hot_Spots.
Much of crime mapping is devoted to detecting high-crime-density areas known as hot spots. Hot spot analysis helps police identify these high crime areas, the types of crime being committed, and the best way to respond. This report discusses hot spot analysis techniques and software and indicates when to use each one. The visual display of a crime pattern on a map should be consistent with the type of hot spot and possible police action. For example, when hot spots are located at specific addresses, a dot map is more precise and thus more appropriate than an area map. Chapters progress in sophistication from novice to advanced, concluding with information for highly experienced analysts.

POLICE FOUND. CRIME MAPPING AND PROBLEM ANALYSIS LAB., CMTY. ORIENTED POLICING SERVICES, CRIME ANALYSIS AND CRIME MAPPING INFORMATION CLEARINGHOUSE (8TH EDITION), https://www.hsdl.org/?view&did=478405.
The clearinghouse provides a comprehensive list of bibliographic and internet resources that may be useful to practitioners and researchers interested in the disciplines of problem analysis, crime analysis, and crime mapping. The bibliographic references are composed of books, articles, and reports that relate to topics such as crime analysis, problem solving, geographic information systems (GIS), crime mapping, and Internet mapping. This particular edition includes over 130 new references and two new resource categories including "Journey to Crime" and "Crime Forecasting." The internet resources provided at the end of the document include links to additional sources of information concerning crime analysis and crime mapping.

RACHEL BOBA, CMTY. ORIENTED POLICING SERVICES, INTRODUCTORY GUIDE TO CRIME ANALYSIS AND MAPPING (2001), https://cops.usdoj.gov/RIC/Publications/cops-w0273-pub.pdf.
This guide was developed from the 2001 curriculum of the "Introduction to Crime Analysis Mapping and Problem Solving" training course conducted by members of the Police Foundation's Crime Mapping Laboratory. It functions both as a "starter" guidebook for persons entering the field and as a reference manual

for current crime analysts or other law enforcement analysts. Topics include types of mapping (single vs. graduated); types of data (tabular vs. geographic); and numerous aspects of data (management, timeliness, validity, reliability, transfer, and privacy).

RACHEL BOBA, CRIME ANALYSIS DEFINED *in* CRIME ANALYSIS AND CRIME MAPPING 5-18 (1st ed. 2005), https://www.sagepub.com/sites/default/files/upm-binaries/6243_Chapter_2__Boba_Final_PDF_2.pdf
This chapter provides an overview of the key definitions and concepts in the field of crime analysis. The components of crime analysis include the collection, collation, and analysis of data; dissemination of results; and incorporation of feedback from users of the information. Types of crime analysis include intelligence analysis (surveillance, wiretapping, informants); criminal investigative analysis (formerly "criminal profiling"); tactical crime analysis (how, when, and where criminal activity has occurred); strategic crime analysis (identify long-term problems in crime and police responses to them); and administrative crime analysis (present interesting findings of crime research and analysis to administration, city government, and citizens).

RACHEL BOBA, INTRODUCTION TO CRIME MAPPING *in* CRIME ANALYSIS AND CRIME MAPPING 37-47 (1st ed. 2005), https://www.corwin.com/sites/default/files/upm-binaries/6244_Chapter_4__Boba_Final_PDF_3.pdf.
Ever since maps have been available that depict the geographic features of communities, such as streets and city boundaries, police departments have used such maps to determine patrol areas and emergency routes as well as to assist patrol officers in finding specific addresses. Police departments have also mapped crime, a process that, until recently, involved the manual placement of pins on hand-drawn wall maps. This chapter discusses the emergence of computerized crime mapping as a tool for conducting crime analysis. It begins with an introduction to key terms and then describes basic concepts before presenting a history of crime mapping and information on the field's current status and career paths.

II. Crime Fighting Technology

AM. REGISTRY FOR INTERNET NUMBERS, https://www.milestonesys.com/globalassets/marketplace/uploaded-assets/0010o00001uxmxfqay/ss_cit_cityofhartford_73502_en_1908_lo.pdf (last visited Nov. 19, 2020).
This website will allow users to look up who owns an IP address.

AXIS COMMUNICATIONS, MAKING THE CITY SAFER WITH SMART CRIME-BUSTING TECHNOLOGY, https://www.milestonesys.com/globalassets/marketplace/uploaded-assets/0010o00001uxmxfqay/ss_cit_cityofhartford_73502_en_1908_lo.pdf.
Like many metropolitan cities, Hartford Connecticut has struggled to sift through and timely analyze the overwhelming amount of crime data collected by its various investigative technologies. This report details the efforts of Harford's law enforcement community to find a solution integrate these technologies, and modernize the city's approach to police work.

BINDB, https://www.bindb.com (last visited Nov. 19, 2020).
This website allows users to look up who owns a credit card number.

Tammy Waitt, *Fort Myers Police Select NC4 Street Smart to Help Fight Crime*, AM. SEC. TODAY (Apr. 5, 2018), https://americansecuritytoday.com/fort-myers-police-select-nc4-street-smart-help-fight-crime/.
The Fort Myers Police Department protects a population of over 77,000 residents and is the county seat and commercial center of Lee County, Florida. This article details their use of NC4 Street Smart, where 206 sworn officers have been equipped with the sophisticated technology and critical resources needed to reduce crime and contribute to the safety of the community. This equipment provides law enforcement organizations with a powerful suite of tools including a crime-fighting blog; bulletin management; map viewer; case management; data feeds; historical crime records; CAD data; repeatable controls; language localization; and advanced search.

WILLIAM SCHWABE ET AL., RAND CORP., CHALLENGES AND CHOICES FOR CRIME-FIGHTING TECHNOLOGY: FEDERAL SUPPORT OF STATE AND LOCAL LAW ENFORCEMENT (2001), https://www.rand.org/pubs/monograph_reports/MR1349.html#download.
This report provides findings of a study of technology in use or needed by law enforcement agencies at the state and local level, for the purpose of informing federal policymakers as they consider technology-related support for these agencies. In addition, it seeks to characterize the obstacles that exist to technology adoption by law enforcement agencies and to characterize the perceived effects of federal assistance programs intended to facilitate the process. The study findings are based on a nationwide Law Enforcement Technology Survey and a similar Forensics Technology Survey conducted in late spring and early summer2000, interviews conducted throughout the year, focus groups conducted in autumn 2000, and review of an extensive, largely nonacademic literature.

III. Cyber Organized Crime

BRUCE NIKKEL, FINTECH FORENSICS: CRIMINAL INVESTIGATION AND DIGITAL EVIDENCE IN FINANCIAL TECHNOLOGIES (2020), https://www.digitalforensics.ch/nikkel20.pdf.
This paper describes an emerging sub-discipline of digital forensics covering financial technologies, or Fintech. The digital transformation of society is introducing new Fintech for payments, funds transfer, and other financial transactions. Criminals are using and abusing financial technologies for fraud, extortion, money laundering, and financing activity in the criminal underground. The investigation of Fintech and digital payment activity needs to be recognized as a new technical sub-discipline of the digital forensics landscape.

CIPHERTRACE, CRYPTOCURRENCY ANTI-MONEY LAUNDERING REPORT (2018), https://ciphertrace.com/crypto-aml-report-2018q3.pdf.
This resource examines the use of cryptocurrency by criminal organizations involved in money laundering. It focuses on cryptocurrency money laundering and does not detail threats to ordinary citizens and the financial system that are rapidly emerging in the blockchain security stack.

GIACOMO PERSI PAOLI ET AL., BEHIND THE CURTAIN: THE ILLICIT TRADE OF FIREARMS, EXPLOSIVES AND AMMUNITION ON THE DARK WEB (2017), https://www.rand.org/pubs/research_reports/RR2091.html.
The overall aim of the study was to estimate the size and scope of the trade in firearms and related products on crypto-markets, including the number of dark web markets listing firearms and related products and services for sale, and the range and type of firearms and related products advertised and sold on crypto-markets.

Revital Sela-Shayovitz, *Gangs and the Web: Gang Members' Online Behavior*, 28(4) J. Contemporary Crim. J. 389 (2012), shorturl.at/jvJKT.
There is a lack of research on gang members' online behavior. The present study addresses this shortcoming by examining how gang members proactively use the Internet. Data were collected by means of in-depth, semi-structured interviews with gang members. In addition, based on reports of gang members, the analysis focused on their group activity on the web. The findings reveal that the Internet does neither play a role in gang formation nor promote considerable changes in group traditional delinquency. However, it does influence socializing processes: Youths who have high-level computer knowledge provide guidance to others, which increases online delinquency. Moreover, the level of computer skills is a key factor in gang involvement in cybercrime: for gangs with members who have high-level computer skills, online delinquency becomes a routine part of the gang's life, and interaction with other groups around the globe facilitates their involvement in cybercrime.

Susan W. Brenner, *Organized Cybercrime - How Cyberspace May Affect the Structure of Criminal Relationships*, 4 N.C. J.L. & TECH. 1 (2002), http://scholarship.law.unc.edu/ncjolt/vol4/iss1/4.
The issue considered in this article is whether what is true of traditional crime is likely to also be true of cybercrime, which deviates from the traditional model of crime in several ways. Section II of this article examines reasons why organized activity has emerged as an aspect of real-world crime. More precisely, it considers the advantages organization offers for real- world criminals. Section III then considers whether these advantages translate to cybercrime. If they do translate, we can expect to see the emergence of organized

cybercriminal activity analogous to that encountered in the real world; that is, we can anticipate the emergence of cybercrime Mafias and cybercrime cartels. To the extent that these advantages do not translate to cybercrime, we may see a very different pattern emerge; organization may prove to be a less significant feature of cybercrime than of real-world crime or it may take quite different forms than those found in real-world crime.

IV. Digital Evidence Investigations

***Courses,* Nat'l Computer Forensics Inst., https://www.ncfi.usss.gov/ncfi/pages/courses.xhtml?dswid=-6771 (last visited Nov. 18, 2020).**
The Secret Service's National Computer Forensics Institute contains free trainings for law enforcement and prosecutors regarding forensic examinations of computers and cellphones.

Eoghan Casey, Digital Evidence and Computer Crime (3rd ed. 2011).
This publication provides the knowledge necessary to uncover and use digital evidence effectively in any kind of investigation. It offers a thorough explanation of how computer networks function, how they can be involved in crimes, and how they can be used as a source of evidence. In particular, it addresses the abuse of computer networks as well as privacy and security issues on computer networks.

Eoghan Casey, Handbook of Digital Forensics and Investigation (1st ed. 2009).
This publication builds on the success of the *Handbook of Computer Crime Investigation*, bringing together renowned experts in all areas of digital forensics and investigation to provide the consummate resource for practitioners in the field. It is also designed as an accompanying text to *Digital Evidence and Computer Crime*.

Humaira Arshad et al., Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence, 14(2) J. Info. Processing Sys. 326 (2018), https://rb.gy/5yw6tb.
Digital forensics is a vital part of almost every criminal investigation given the amount of information available and the opportunities offered by electronic data to investigate and evidence a crime. However, in criminal justice proceedings, these electronic pieces of evidence are often considered with the utmost suspicion and uncertainty, although, on occasions are justifiable. This article presents a comprehensive study to examine the issues that are considered essential to discuss and resolve, for the proper acceptance of evidence based on scientific grounds. Moreover, the article explains the state of forensics in emerging sub-fields of digital technology such as, cloud computing, social media, and the Internet of Things, and reviewing the challenges which may complicate the process of systematic validation of electronic evidence.

Karen Kent et al., Nat'l Inst. of Standards and Tech., Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response (2006), https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf.
This guide provides general recommendations for performing the forensic process. It also provides detailed information about using the analysis process with four major categories of data sources: files, operating systems, network traffic, and applications. The guide focuses on explaining the basic components and

characteristics of data sources within each category, as well as techniques for the collection, examination, and analysis of data from each category. The guide also provides recommendations for how multiple data sources can be used together to gain a better understanding of an event.

Kim-Kwang Raymond Choo & Ali Dehghantanha, Contemporary Digital Forensic Investigations of Cloud and Mobile Applications (2017).
This publication comprehensively discusses the implications of cloud (storage) services and mobile applications on digital forensic investigations. The book provides both digital forensic practitioners and researchers with an up-to-date and advanced knowledge of collecting and preserving electronic evidence from different types of cloud services, such as digital remnants of cloud applications accessed through mobile devices.

Nat'l Inst. of Just., Off. of Just. Programs, U.S. Dep't of Just., Electronic Crime Scene Investigation: A Guide for First Responders (2nd ed. 2008), https://www.ncjrs.gov/pdffiles1/nij/219941.pdf.
This guide is intended to assist State and local law enforcement and other first responders who may be responsible for preserving an electronic crime scene and for recognizing, collecting, and safeguarding digital evidence. It is not all inclusive but addresses situations encountered with electronic crime scenes and digital evidence.

Nat'l Inst. of Just., Off. of Just. Programs, U.S. Dep't of Just., Investigations Involving the Internet and Computer Networks (2007), https://www.ncjrs.gov/pdffiles1/nij/210798.pdf.
This report was developed by the Technical Working Group for the Investigation of High Technology Crimes and is intended to be a resource for individuals responsible for investigations involving the Internet and other computer networks.

Nat'l Inst. of Just., Off. of Just. Programs, U.S. Dep't of Just., Investigative Uses of Technology: Devices, Tools, and Techniques (2007), https://www.ncjrs.gov/pdffiles1/nij/213030.pdf.
This special report is intended to be a resource to any law enforcement personnel (investigators, first responders, detectives, prosecutors, etc.) who may have limited or no experience with technology-related crimes or with the tools and techniques available to investigate those crimes. It is not all inclusive. Rather, it deals with the most common techniques, devices, and tools encountered.

***Published*, Sci. Working Grp. on Dig. Evidence, https://www.swgde.org/documents/published (last visited Nov. 18, 2020).**
This website is a repository of documents crafted by the Scientific Working Group on Digital Evidence—from best practices for archiving digital media, to best practices for mobile device evidence collection and preservation.

Sean E. Goodison et al., RAND Corp., Digital Evidence and the U.S. Criminal Justice System (2015), https://www.rand.org/pubs/research_reports/RR890.html.

This report describes the results of a National Institute of Justice-sponsored research effort to identify and prioritize criminal justice needs related to digital evidence collection, management, analysis, and use. It asks three questions: 1) What is the state of digital evidence today?; 2) What are the criminal justice needs associated with digital evidence collection, management, analysis, and use?; and 3) What are the highest priorities among those needs?

Webinar by Cathee Hansen, Chris Gray & Adam Bechtold, *Digital Evidence Part I: The Investigative Stage – Recognition, Collection, Search,* AEQUITAS, https://aequitasresource.org/resources/ (recorded Sept. 18, 2020).
This two-part webinar series presented by the Denver District Attorney's Office, in partnership with AEquitas, explores the scope of data available from sources of digital evidence and strategies on how such data can effectively be developed with forensically-sound practices. Presenters discuss theories of admission, rules of evidence, and "real life" examples to demonstrate how to properly authenticate and introduce digital evidence in court proceedings. Part I of the series explores the different types and sources of electronic data that are available to investigators; how such data can be properly collected, regardless of whether it is in a physical device or electronic records; and methods to facilitate searching and seizing data.

Webinar by Cathee Hansen, Chris Gray & Adam Bechtold, *Digital Evidence Part II: Now That You've Got It and Can Read It, What Can You Do With It?,* AEQUITAS, https://aequitasresource.org/resources/ (recorded Sept. 25, 2020).
This two-part webinar series presented by the Denver District Attorney's Office, in partnership with AEquitas, explores the scope of data available from sources of digital evidence and strategies on how such data can effectively be developed with forensically-sound practices. Presenters discuss theories of admission, rules of evidence, and "real life" examples to demonstrate how to properly authenticate and introduce digital evidence in court proceedings. Part II of the series discusses how legally-obtained data can be analyzed, depending on the type of data in question. Presenters also discuss strategies for effectively presenting data at trial.

Webinar by Jane Anderson, *#GUILTY: Identifying, Preserving, and Presenting Digital Evidence,* AEQUITAS, https://aequitasresource.org/resources/ (recorded Nov. 28, 2017).
Unfortunately, as technology becomes more integral to our lives, offenders increasingly misuse technology to facilitate crimes against women, and as a means to assert power and control in the course of an intimate partner relationship. This webinar demonstrates how cyber investigations can be used to reveal evidence of criminal activity, as well as evidence of the power and control dynamics of an abusive relationship. The presenter discusses theories of admission, rules of evidence, and case law using "real life" examples to demonstrate how to properly authenticate and introduce digital evidence in civil and criminal proceedings.

V. Digital Preservation Orders

Fernando Molina Granja & Glen D. Rodriguez Rafael, *The preservation of digital evidence and its admissibility in the court,* 9(1) INT'L J. ELEC. SEC. & DIGIT. FORENSICS 1 (2016), https://www.researchgate.net/publication/312665626_The_preservation_of_digital_evidence_and_its_admissibility_in_the_court.
This article's objective is to screen and analyze the common models of digital preservation that exist, the elements, the degree of compliance with the general guidelines, the use of techniques and compliance with specific requirements as well as to evaluate the need for a solution to the environment of criminal investigation institutions, in the scenario that lacks a specific model.d

Mike Kastellec, *Practical Limits to the Scope of Digital Preservation,* 31(2) INFO. TECH & LIBRARIES 63 (2012), https://ejournals.bc.edu/index.php/ital/article/view/2167.
This paper examines factors that limit the ability of institutions to digitally preserve the cultural heritage of the modern era. The author takes a wide-ranging approach to shed light on limitations to the scope of digital preservation. He finds that technological limitations to digital preservation have been addressed but still exist, and that non-technical aspects—access, selection, law, and
finances—move into the foreground as technological limitations recede. The paper proposes a nested model of constraints to the scope of digital preservation and concludes that costs are digital preservation's most pervasive limitation.

VI. Electronic Discovery

Jenia I. Turner, *Managing Digital Discovery in Criminal Cases*, 109 J. CRIM. L & CRIMINOLOGY 237 (2019), https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7651&context=jclc.
Though the burdens and challenges of discovery—especially electronic discovery—are usually associated with civil rather than criminal cases, this is beginning to change, and is already common in white-collar crime cases, where voluminous digital discovery is increasingly a feature of ordinary criminal prosecutions. This article examines the explosive growth of digital evidence in criminal cases and the efforts to manage its challenges and makes three key claims regarding criminal case electronic discovery: (1) the volume, complexity, and cost of digital discovery will incentivize the prosecution and the defense to cooperate more closely; (2) cooperation between the parties will not be sufficient to address the serious challenges that digital discovery presents to the fair and accurate resolution of criminal cases; and therefore (3) digital discovery in criminal cases needs to be regulated more closely.

KRISTINE HAMANN, PROSECUTORS' CTR. FOR EXCELLENCE, THE BENEFITS OF ELECTRONIC DISCOVERY: CASE STUDY (2018), https://pceinc.org/wp-content/uploads/2019/11/20180218-King-County-Discovery-Final-with-Appendix-and-cover3-3.pdf.
Prosecutors are obligated to provide timely and complete discovery, particularly with regard to exculpatory and impeachment material. The discovery process can be complex and time consuming. Failure to properly record discovery documents provided to the defense can jeopardize cases and put prosecutors at risk of being charged with ethical violations. Thus, prosecutors are turning to technology to streamline the discovery process and to create a reliable record of what was turned over to the defense and when. This report discusses the electronic discovery system developed by the King County Prosecuting Attorney's Office, located in Seattle, Washington. The report includes examples of the correspondence given when discovery requests have been received.

Webinar by Jane Anderson & Meg Garvin, *Safeguarding Victim Privacy in a Digital World: Ethical Considerations for Prosecutors,* AEQUITAS, https://aequitasresource.org/resources/ (recorded May 18, 2017).
Prosecutors have an obligation to provide to the defense all evidence in the government's possession or control that is material to a defendant's guilt or punishment. How can we fulfill that obligation, while at the same time safeguarding victim privacy against unnecessary disclosure? In the digital age, these cases present unique ethical challenges related to privacy and confidentiality, prosecutorial discretion, recantation, and disclosure of evidence. This presentation uses hypothetical case scenarios to: address ethical considerations in the context of the investigative function of prosecutors, digital evidence, discovery obligations, and immunity; identify confidential, privileged, non-material, and/or irrelevant victim information and records; discuss threshold requirements for defense attempts to obtain information or for in camera review; introduce pretrial and trial strategies that support the protection of victim privacy, including collaboration with allied professionals.

VII. Investigation and Prosecution Sample Tools

Note: AEquitas has various other sample tools available upon request—including preservation letters, non-disclosure orders, motions to compel passcodes, and responses to motion to compel victim cell phones and social media—in addition to related case law.

Call Detail Records Affidavit in Support of Search Warrant, Denver Dist. Attorney's Off. (on file with AEquitas).
This is a sample affidavit template to support a search warrant and court order for production of call detail records.

Call Detail Records Search Warrant, Denver Dist. Attorney's Off. (on file with AEquitas).
This is a sample search warrant template for call detail records.

Cell Phone Consent to Search Form, Memphis Police Dept. (on file with AEquitas).
This is a sample consent to search form utilized by Memphis Police Department when requesting access to a cell phone or electronic storage device. It is used to request consent to search from non-fatal overdose victims and from the parents/guardians of fatal overdose victims who are minors.

Cell Phone Data Affidavit in Support of Search Warrant, Denver Dist. Attorney's Off. (on file with AEquitas).
This resource is a sample affidavit template to support a search warrant regarding access to data stored in a cell phone.

Cell Phone Data Search Warrant, Denver Dist. Attorney's Off. (on file with AEquitas).
This resource is a sample search warrant template regarding access to cell phone records — including precise location data and substantive messaging information.

Cellular Device Tracking Form, Memphis Police Dept. (on file with AEquitas).
This is a sample form used by Memphis Police Department personnel to track the chain of custody for a cellular device in their possession.

Facebook User Records Affidavit in Support of Search Warrant, Denver Dist. Attorney's Off. (on file with AEquitas).
This resource is a sample affidavit to support a search warrant and court order for production of records regarding a specific Facebook account — including activity logs and all IP address data.

Facebook User Records Search Warrant, Denver Dist. Attorney's Off. (on file with AEquitas).
This resource is a sample search warrant and court order for production of records regarding a specific Facebook account.

KING COUNTY'S SEARCH WARRANT RSCH. CTR., https://ingress.kingcounty.gov/Login/ (last visited Nov. 19, 2020).
This website contains lots of sample search warrants, available to law enforcement and prosecution personnel.

N.Y. Prosecutors Training Inst., https://www.nypti.org (last visited Nov. 19, 2020).
This repository, maintained by the District Attorneys Association of New York, contains lots of sample search warrants.

VIII. Social Network Analysis (SNA)

INT'L ASS'N OF CRIME ANALYSTS, SOCIAL NETWORKING ANALYSIS FOR LAW ENFORCEMENT (2018), https://crimegunintelcenters.org/wp-content/uploads/2018/07/iacawp_2018_02_social_network_analysis.pdf.
This document focuses on Social Network Analysis (SNA), and its role in helping us understand criminal networks, co-offending patterns, and victimization. Primarily, the usefulness of SNA to law enforcement hinges on the fact that knowing who a person associates with (whether s/he be a suspect, victim, or potential witness) can aid in predicting that person's future movements. It is well documented that crime and victimization are not randomly distributed across people or space. In addition, victims and offenders are often connected in multiple ways and play varying roles in criminal events (such as a victim, offender, co-offender, or witness—often swapping in different events) and in daily social life (such as an acquaintance, family member, spouse/partner, etc.).

***Social Media Reference Guide*, Fed. Bureau of Investigations, https://crimegunintelcenters.org/wp-content/uploads/2018/07/Social-Media-Guide-For-Investigations-07272017.pdf (last visited Oct. 7, 2020).**
This guide offers a collection of over one hundred web sites pertaining to social networking. Topic areas include operations security (OPSEC); anonymization; website evaluation; people searching; social networking in general; blogging tools; specific social networks (Facebook, Twitter, Instagram); image, file, and video sharing; analytical tools; and additional miscellaneous web sites.

Webinar by RTI International, *IPS Learning Community Series: Social Network Analysis,* AEQUITAS, https://aequitasresource.org/resources/ (recorded July 22, 2020).
As home to the Innovative Prosecution Solutions (IPS) Research and Evaluation Training and Technical Assistance team, RTI International has developed a webinar series to support the creation and ongoing engagement of a learning community of local researchers and practitioners interested in discussing evaluation-related topics, sharing methodological techniques, and addressing problem-solving challenges in carrying out applied research. In the fourth webinar in the series, research partners from two IPS Projects discussed how they are utilizing — or plan on utilizing – social network analysis (SNA) to aid in action research. View the discussion to learn more about the basics of SNA and how it can be used to better understand the relationships between opioid manufacturers, distributors, and overdose victims.