PI magazine .com

professional investigator magazine

$9.95

November/December 2025

RECOGNIZING AND PREVENTING WORKPLACE VIOLENCE

A Guide for Companies and Private Investigators

THE ART OF THE SIGN UP
What Investigators Should Know When Handling a New Case

SURVEILLANCE IN MODERN INVESTIGATIONS
A Perspective from the Field

THE SURROGATE SECURITY DIRECTOR CHECKLIST

THE TRUST FACTOR
Elevating the Investigative Interview Beyond Technique

DEPARTMENTS

IN EVERY ISSUE

Retention, Access, and Protection of Vital Data

BY **ROBERT B. FRIED** AND **SHEVACH BERKOVITS**

As we navigate this technological world, we leave behind digital footprints. However, because of the significant volume of data generated every second of every day, we cannot store all of it forever. Today, investigations often involve large volumes of electronic evidence from a variety of data sources. We must understand how storing and maintaining data can affect its lifecycle. It is also important to acknowledge that data sources come with varying considerations based on whether the sources are owned or managed by individuals, corporations, or government entities.

NAVIGATING THE COMPLEXITIES OF DATA STORAGE & HYGIENE

Data storage is possible on physical devices, on physical media, or in the cloud. Regardless of the storage location, remember that data is inherently fragile. For example, hard disk drives can store data for extended periods; however, they can fail because of mechanical issues, causing data to be inaccessible or non-recoverable. A mobile device may temporarily store data before deleting it, as another example. With ephemeral messaging, users may take a screenshot of the messages before they disappear, therefore saving it elsewhere! When we have a choice, deciding what data to save versus what to delete can be a daunting task.

Although devices have considerable storage capacities, you can never have enough! Maintaining good data hygiene is important, not only to preserve that precious storage space, but because it is necessary (i.e., corporations in a regulated industry must maintain specific data for a defined period). To assist with balancing our data storage habits, devices, and apps, service providers may have configuration settings or enforced policies that determine what happens to data and when. It may or may not be possible for users to change settings or relax policies. For instance, mobile device management (MDM) solutions often secure mobile devices used for business to protect the device's data. It is necessary for digital forensics practitioners to coordinate with legal and IT to preserve or collect the device's data.

NOT JUST PERSONAL OR PRIVATE (SECTOR)

Data retention also applies to data sources leveraged by government entities, including law enforcement agencies. The availability of information stored in databases is crucial for investigations. There are databases at the federal, state, and local levels that store specific information for defined periods.

One example of a law enforcement records keeping database for constant and immediate access is the New York State's eJustice Integrated Justice Portal ("eJusticeNY"). The Portal is a secure extranet system administered by the New York State Police, providing access to all available public safety, criminal justice, and civil data information. Retention policies for records within eJusticeNY include two (2) years for articles, five (5) years for boats, license plates, securities, vehicles, and indefinite entries for wanted, missing, and unidentified persons.

Another example of a law enforcement records keeping database is the open-source FBI Crime Data Explorer (CDE) through its Uniform Crime Reporting (UCR) Program. The FBI's UCR Program manages the CDE and is an interactive online public tool to help better understand the massive amounts of crime data. Said data includes violent (e.g., murder, manslaughter, rape, and robbery) and property (e.g., burglary, larceny, and arson) crime. Since its earliest iteration in 1930, the CDE provides estimated data from over 18,000 federal, state, county, local, tribal, territorial, and university law enforcement agencies via its National Incident-Based Reporting System (NIBRS), simplified by victims, offenders, property involved, and arrestees. The CDE's retention policies include automated data verification, ensuring conformity to strict program compliance and national standard formats.

New York legislation granted accessibility to governmental data-

bases under the Public Officer's Law, or the Freedom of Information Law (FOIL), mandating that all records are subject to disclosure, barring statute exemptions including juvenile, personnel, sealed, sex victim, and youthful offender records. An agency must acknowledge inquiries within five (5) business days, determine access within twenty (20) business days, and not charge more than $0.25 per page.

WHEN DATA IS UNDER ATTACK

On September 08, 2022, the cyber-attack on Suffolk County, New York, provided a case study for failing to initiate and maintain a data resilience response and recovery plan. The ransomware group BlackCat (also known as ALPHV or Noberus) gained access to the municipality's entire technology infrastructure. Later, vital data was identified on the dark web, including network maps, budgets, credentials, passwords, and personal-identifying information. The initial ransom demand was $2.5 million, later reduced to $650,000, but eventually cost the county $25 million in response and remediation. The failures ranged from the lack of coordination among the different IT units, the absence of a resilience plan, the lack of a chief information security officer (CISO), insufficient staffing and training, and minimal protection against lateral movement. Incidentally, it was discovered that departmental firewalls had reached their end-of-life five (5) years prior.

SECURING DATA FOR THE FUTURE

Today, we generate and rely heavily on large volumes of data from various sources. Configuration settings and policies dictate how we store and maintain data. Having good data hygiene (i.e., effective data retention policies) and a resilient security posture (i.e., implementing robust incident response and disaster recovery plans) is crucial in protecting our vital information against threats, and for ensuring future access and use – especially when it matters the most. **PI**

REFERENCES

1. FBI Uniform Crime Reporting Program. 2023. "About the Crime Data Explorer." FBI Crime Data Explorer. FBI.gov. 2023. https://cde.ucr.cjis.gov/LATEST/webapp/#/pages/about.
2. Harrington, Mark. 2024. "Suffolk County Cyberattack Recovery Costs Hit $25M." Newsday. August 5, 2024. https://www.newsday.com/long-island/suffolk/suffolk-cyberattack-costs-romaine-bellone-ulul94lm.
3. Nassau County Police Department. 2000. "Department Procedure OPS 4215: Freedom of Information Requests." August 18, 2000.
4. New York State. 2025. "NYS Integrated Justice Portal." EJusticeNY. 2025. https://www.ejustice.ny.gov.
5. New York State Senate. 2014. "Article 6: Freedom of Information Law Public Officers." Nysenate.gov. September 22, 2014. https://www.nysenate.gov/legislation/laws/PBO/A6.
6. NYS eJusticeNY. 2011. "Integrated Justice Portal: Use & Dissemination Rules & Regulations." Albany, NY: NYS eJusticeNY.
7. Suffolk County Legislature. 2024. "Report on the 2021-2022 Cyber-Attack on Suffolk County." Suffolk County, NY Legislature. Special Cyber Intrusion Investigation Committee. https://www.scnylegislature.us/DocumentCenter/View/118502/09122024-Report-On-The-2021-2022-Cyber-Attack-On-Suffolk-County-PDF.

Robert B. Fried is an accomplished expert with decades of experience performing data collections and forensic investigations of electronic evidence. He attained a BS and MS in Forensic Science from the University of New Haven. He holds and actively maintains industry certifications and is a licensed PI in Michigan, New York, and South Carolina. Robert serves on the Board of Advisors for the Masters in Investigations program at the University of New Haven, the Global Advisory Board for EC-Council's CHFI certification and is a Fellow at 1he Henry C Lee Institute of Forensic Science at the University of New Haven. He is the author of the books: Forensic Data Collections 2.0: A Selection of Trusted Digital Forensics Content and Forensic Data Collections 2.0: The Guide for Defensible & Efficient Processes.

Shevach Berkovits holds a Doctorate in Homeland Security and a B.S. in Criminal Justice from St. John's University in New York, and a M.A. in Communications from the New York Institute of Technology. His research focuses include risk assessment and management in policing, police reform, police training, and resilience. Additionally, Dr. Berkovits has conducted extensive research on community policing and the development of training programs that enhance the relationship between law enforcement and the communities they serve. He is an active law enforcement officer with over 17 years of experience, bringing both academic insight and practical expertise to his work.