Protect hard-won documents from theft, breakdowns and the government

You went through all that work to acquire public records and data, haggling for months or years with stubborn officials, and huzzah! You discovered the smoking gun that will expose corruption and win the Pulitzer.

And then the government raids your home. Or malware corrupts your data. Or your laptop takes a dip in the pool.

Protecting records is a step we often overlook. Sure, if you lose them, you can retrieve them from the government. But what a hassle. And what if the government wants to know what you are working on?

By **David Cuillier**, *Brechner Freedom of Information Project*

Invasion of the record snatchers

In the past year, we've seen some brutal assaults on press freedom by the government raiding journalists' computers:

- In May, FBI agents entered freelance journalist Tim Burke's home in Tampa, Florida, seizing computers, hard drives and a cell phone. Burke was working on a story about Tucker Carlson, using unaired video Burke had obtained from a publicly accessible website. In September, a federal magistrate ruled that the government doesn't have to return the materials, his attorney Mark Rasch told me. Even the affidavit justifying the raid may be kept secret.
- In July, Kenwyn Caranna, a reporter for the Greensboro News & Record, was covering a juvenile court hearing when a judge seized her notes and told her she couldn't write about the hearing. Executive Editor Dimon Kendrick-Holmes said in an email that the newspaper is challenging the gag order and requesting the unsealing of the notes, with a possible resolution in January.
- In August, police in Marion, Kansas, seized computers, cell phones and documents at the Marion County Record and at the publisher's home — for allegedly acquiring a DUI record in violation of the Driver Privacy Protection Act. Turns out the records came from a public website. The police chief has since been suspended and reporter Debbie Gruver, who was investigating the police chief, is suing in federal court, saying the raid infringed on her constitutional rights.

In 2022, three other journalists in the United States had their equipment seized by the government, according to the U.S. Press Freedom Tracker (pressfreedomtracker.us). In previous years, few, if any, journalists reported these affronts to the First Amendment.

Safe document storage

Sure, odds are low the government will raid your home, but it can't hurt to protect what you acquired from any number of file catastrophes — theft, fire or hard drive crash.

Martin Shelton, principal researcher at the Freedom of the Press Foundation, recommends the following:

1. Encryption software is easy to use, such as FileVault for Macs and BitLocker for Windows. Linux Unified Key Setup (LUKS) can encrypt USB drives.
2. Cell phones already come with encryption — just make sure the password is beefy.
3. In general, Shelton says, use long, random passwords, and different passwords for each account. Try a password manager, like 1Password for Journalism (free). Newsrooms should require two-factor authentication for accessing project management software and data.
4. Back up your files on a hard drive in a different location from your newsroom or home, or to the Cloud. Macs can use Time Machine.

Shelton said the most important measure is to have different passwords — not the same one used for everything. A physical notebook listing them is fine, as long as it is safe. He also suggested that paper files be digitized quickly.

"This is about workplace continuity," Shelton said. "If I have backups of all my devices, and it's safe, I am no longer worried whether it's lost, stolen or breaks down."

More advice can be found in a new journalists' guide to search warrants, produced by the Freedom of the Press Foundation and Florida First Amendment Foundation (tinyurl.com/raidaid). ◆

David Cuillier, Ph.D. (he/him), is director of the Joseph L. Brechner Freedom of Information Project at the University of Florida and co-author of "The Art of Access: Strategies for Acquiring Public Records." He can be reached at cuillierd@ufl.edu.