Published on *The National Law Review* https://natlawreview.com

Why Dumping Sensitive Data on Network Shares is a Liability

Article By:

Kathryn M. Rattigan

Jim Merrifield, IGP, CIGO

Are you storing sensitive data on a shared network drive? If so, your organization could be at serious risk of a data breach or privacy lawsuit. Shared drives, like the common “S:\ drive,” are often used to store documents, spreadsheets, customer information, financial records, and even scanned IDs. But here’s the problem: these network shares are rarely encrypted, lack clear data governance policies, and are accessible to dozens—or even hundreds—of employees across different departments. Without proper oversight, unsecured network drives become a data security nightmare.

Don’t let poor information governance put your business at risk; take the time to learn why securing sensitive data on shared drives is critical for avoiding data breaches, maintaining compliance with privacy laws, and safeguarding your company’s reputation.

In today’s environment of rapidly expanding state consumer privacy laws and data breach notification statutes, companies that fail to control where sensitive data lives are sitting on serious legal and reputational risk. Here’s what you need to know—and why unsecured network shares are no longer just an IT headache. It’s a legal liability.

The Rise of State Privacy Laws: More Than Just California

Most people know about California’s Consumer Privacy Act/Consumer Privacy Rights Act, but it’s far from alone. As of 2025, over a dozen states have passed their own consumer privacy laws—including Colorado, Connecticut, Utah, Virginia, Texas, Florida, Oregon, and others. Here’s what these state privacy laws typically grant consumers:

- The right to know what personal data companies collect.
- The right to access or delete their personal data.
- The right to opt-out of data sales or targeted advertising.
- The expectation that their data will be securely protected.

“Reasonably protected” sounds vague, but it’s increasingly being interpreted to mean basic security practices—like encryption, access controls, and data governance. Storing Social Security numbers or financial info in an unprotected shared drive with no audit trail? That’s not going to fly.

Data Breach Notification Laws: 50 States, 50 Triggers

Every U.S. state has its own data breach notification law, and many have recently updated them. These laws require businesses to notify affected consumers—and sometimes regulators—when certain types of personal information are accessed or acquired without authorization.

The trigger? Often, it's exposure of unencrypted data such as:

- Social Security numbers
- Driver's license numbers;
- Financial account or credit card numbers; and
- Health records.

Why Network Shares are High-Risk

If that data lives on an unsecured network share, accessible by anyone on the network—or worse, breached by an outsider—you may have a legal duty to notify, and fast.

Shared network drives are a leftover from a simpler time. They often:

- Lack encryption, either at rest or in transit.
- Have overly broad access (e.g., "Everyone in Finance" means everyone).
- Are unmanaged—no one monitors what's stored, for how long, or by whom.
- Become digital junk drawers: you name it, someone's dumped it there.

In short, they're a soft target for internal mishandling or external breaches.

Even if no breach has occurred yet, regulators may still view careless storage as a failure to implement reasonable security measures, something required by many state laws (and by the FTC under its enforcement of Section 5 for unfair practices).

Real World Risk: Enforcement and Lawsuits

Let's connect the dots:

- A former employee downloads a folder full of unencrypted spreadsheets with customer data from a shared drive and walks out the door.
- A ransomware attacker gains access to your network and hits a file share containing years' worth of sensitive HR or payroll data.
- A privacy audit reveals that your network share is a free-for-all and your company never implemented access logs or retention policies.

In each case, you're potentially looking at:

- Mandatory breach notifications;
- Fines from state attorneys general;
- Consumer lawsuits, including class actions; and
- Reputational damage, especially if the exposure goes public.

What You Can Do Now

The good news? Much of this risk is preventable. Here are some practical steps:

1. Encrypt sensitive data at rest and in transit. Don’t assume your internal network is a safe zone.
2. Limit access based on role or need-to-know. Broad group permissions are a red flag.
3. Inventory your data. You can’t protect what you don’t know you have.
4. Establish a governance policy. Set clear rules about what data can be stored, where, and for how long.
5. Clean up legacy shares. Archive or securely delete outdated files, especially ones with sensitive info.
6. Train employees. They need to know that dumping sensitive info into a shared folder is no longer acceptable.

State privacy laws are becoming more aggressive, and regulators are increasingly focused on where and how companies store consumer data, not just how they use it. An old network share with no encryption, no oversight, and no purpose may seem like low-hanging fruit from a compliance perspective, but it’s exactly the kind of vulnerability that can turn into a legal firestorm.

If your organization hasn’t taken a hard look at its shared storage practices lately, now is the time. Because in the age of modern data privacy laws, “we didn’t know it was there” is no longer a defense.

National Law Review, Volume XV, Number 171