Your Clients Have Estate Plans. Their Digital Lives Probably Don't.

By Michael C. Maschke, Sharon D Nelson, Esq., and John W. Simek

Most people have at least a basic estate plan, a will, maybe a trust, beneficiary designations, and powers of attorney. The traditional pieces are usually there.

What is missing is everything else.

Today, much of a person's life exists entirely in digital form, including financial accounts, payment platforms, photos, documents, cloud storage, loyalty points, and even smart home systems. As a recent SANS OUCH newsletter points out, when someone dies without a plan for those assets, families can face financial disruption, security risks, and the permanent loss of important data.

Digital Assets Are Real Assets

The concept of digital inheritance is no longer theoretical. It is simply the extension of estate planning into modern life. Digital assets can include such things as email accounts, online banking, cryptocurrency wallets, and subscription services.

The problem is that these assets are often invisible. There is no paper trail in a file cabinet. There is no physical key to hand over. Access is controlled by passwords, multi-factor authentication, and platform policies that may not recognize traditional legal authority. This creates a practical problem for families. Even if someone has the legal right to access an account, they may lack the technical ability to do so.

The Risk Is Not Just Inconvenience

When digital assets are not properly planned for, the consequences go well beyond inconvenience.

The SANS guidance highlights several real risks. Families may be unable to access funds or meet ongoing financial obligations. Active accounts can be targeted for takeover or fraud. Important documents and personal memories can be lost entirely.

There is also an emotional component. Unresolved online accounts, social media profiles, and digital identities can cause confusion and distress for loved ones. In some cases, accounts remain active indefinitely, raising privacy concerns and potential security risks.

For law firms advising clients, this is not an issue to overlook. It is a growing category of risk that intersects finance, privacy, and security.

The Law Has Not Fully Caught Up

Part of the challenge is that legal frameworks are still catching up to digital reality.

Traditional estate planning assumes that assets can be identified, valued, and transferred. Digital assets are different. They may be governed by terms of service agreements, subject to licensing restrictions, or controlled by providers that limit access after death.

Even when statutes address digital assets, implementation can be inconsistent. As a result, practical access often depends less on legal authority and more on preparation. In other words, having the right documents is necessary but not always sufficient.

What Lawyers Should Be Doing Differently

The takeaway is not that estate planning needs to become more complicated. It needs to become more complete. There are several practical steps lawyers can incorporate into their process.

First, inventory matters. Clients should identify which digital assets exist, where they are stored, and how they are accessed. Without that baseline, everything else becomes guesswork.

Second, access planning is critical. This does not mean writing passwords in a will. It means using secure mechanisms, such as password managers, digital vaults, or designated access tools, to ensure trusted individuals can access accounts when needed.

Third, clients should designate a digital executor or, at a minimum, provide clear instructions on who will manage digital assets. Traditional fiduciaries may not always have the technical expertise required.

Fourth, platform-level settings should not be ignored. Many major providers now offer legacy contact or account management features that let users define what happens to their data if they are incapacitated or deceased.

Finally, this needs to be part of the conversation. If lawyers are not asking about digital assets, clients are unlikely to raise the issue on their own.

The Bigger Picture

Digital legacy is not just about account access. It is about how identity, memory, and value persist after death. Increasingly, people leave behind not only financial assets but also entire digital footprints that reflect their relationships, history, and personal lives.

That footprint can have lasting meaning for families. It can also pose a risk if unmanaged. In modern estate planning, what you cannot see may be just as important as what you can.

Michael C. Maschke *is the President and Chief Executive Officer of Sensei Enterprises, Inc. Mr. Maschke is an EnCase Certified Examiner (EnCE), a Certified Computer Examiner (CCE #744), an AccessData Certified Examiner (ACE), a Certified Ethical Hacker (CEH), and a Certified Information Systems Security Professional (CISSP). He is a frequent speaker on IT, cybersecurity, and digital forensics, and he has co-authored 14 books published by the American Bar Association. He can be reached at mmaschke@senseient.com.*

Sharon D. Nelson *is the co-founder of and consultant to Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association, and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com.*

John W. Simek *is the co-founder of and consultant to Sensei Enterprises, Inc. He holds multiple technical certifications and is a nationally known digital forensics expert. He is a co-author of 18 books published by the American Bar Association. jsimek@senseient.com.*