AI, Privacy, and Legal Ethics:
Lessons from *23andMe* and the Copyright Wars

What do a genetic testing company and multimillion-dollar copyright lawsuits have to do with your law practice?

Everything.

They show that once you give data to someone else, you may lose ownership. You certainly lose control of it.

www.theformtool.com
info@theformtool.com

Introduction – What *23andMe* and Copyright Battles Teach Us About Security

The recent *23andMe* data breaches exposed the harsh truth of "trusted" platforms: even when customers consented to share their genetic information, they never imagined it would be resold, repurposed, or hacked. Meanwhile, authors and publishers are suing companies for scraping copyrighted material, alleging that once content entered massive training databases, it became part of a black box no one could fully control.

For lawyers, the parallels are unavoidable. Every time you upload a draft, a client questionnaire, or discovery data to a cloud-based document automation or AI tool, you may be giving up more than convenience. You may be surrendering control.

Altman Confirms the Subpoena Risk

Even OpenAI's Sam Altman admits that conversations with ChatGPT lack legal privilege and may be disclosed under subpoena—even in legal contexts. Under a recent New York court order deleted chats may remain available for longer than the contractural 30 days.

If attorney-client style conversations are exposed this way, how can any lawyer claim they're making "reasonable efforts" under Model Rule1.6 when using cloud tools?

The only reliable way to ensure confidentiality is to keep client data entirely under the attorney's direct control.

Lesson One – Control of Data Is Hard to Reclaim

The *23andMe* breach is a cautionary tale. Customers believed their DNA profiles were private, but once stored on a third-party server, their data became a commodity—licensed, analyzed, and ultimately exposed.

The moment you share data with someone else, you lose practical control over how it's stored, accessed, and used.

The same is true for attorneys relying on cloud-based document assembly or AI drafting tools. Many Terms of Service grant the vendor broad rights to store, replicate, and even analyze uploaded documents. Once in their hands, your client's contracts, pleadings, or estate plans could be copied, archived, or mined in ways you can't monitor—and often can't stop.

Lesson Two – "Fair Use" vs. "Ownership" in the Copyright Wars

AI companies defend mass ingestion of copyrighted material as "transformative use," but authors argue it's wholesale copying under another name. These lawsuits, led by The New York Times and high-profile authors, hinge on a simple question: does the right to "use" data include the right to repurpose and resell it?

For lawyers, the answer should be obvious: No. Yet many legal tech tools treat uploaded documents exactly this way, using them to "improve services" or train future models.

Even if anonymized, patterns from privileged client documents can become part of an AI model's "memory." That creates a genuine risk: what happens if fragments of one client's confidential language surface in another user's work product? Even worse, what if it's client data?

Lesson Three – Legal Ethics Demand More Than Vendor Assurances

The ABA's Model Rule 1.6 requires lawyers to make "reasonable efforts" to prevent unauthorized disclosure of client information. But how "reasonable" is it to rely entirely on a vendor's marketing claim or SOC 2 certification when their Terms of Service explicitly allow them to keep, copy, or analyze your files?

Rule 1.6 seems clear: lawyers may not share client information unless the client gives informed consent, disclosure is impliedly authorized for representation, or a narrow exception applies. Even then, Comment 18 requires "reasonable efforts" to prevent unauthorized access or disclosure.

Cloud-based services routinely store, copy, or back up data across multiple jurisdictions and often reserve rights to analyze or anonymize information for "service improvement." These practices push beyond what 1.6 permits because attorneys cannot ensure or control how client data is used once uploaded.

The only way to comply with the spirit—and arguably the letter—of Rule 1.6 is to keep client data entirely within the attorney's direct control.

If there's a breach, ethical and possibly legal liability still rests with the lawyer—not with the vendor.

Once you give data to someone else, you may lose ownership. You certainly lose control of it. That's not just a security issue; it's an ethical one.

A Better Way – Air-Gapped Automation

The simplest solution is also the most secure: don't send the data anywhere in the first place.

TheFormTool® PRO and Doxserá® are built on this principle. They operate entirely offline:

- No internet connection required
- No cloud storage
- No vendor tracking or background communication

Client information never leaves your system, ensuring that control—and ownership—remain exactly where they belong: with you.

Conclusion – The Ethics of Control

The lessons of *23andMe* and the copyright lawsuits are clear. Data has become the world's most valuable currency, and once you hand it over to a third party, it's no longer entirely yours.

For attorneys, that's unacceptable. Once you give data to someone else, you may lose ownership. You certainly lose control of it.

Privacy isn't just a selling point. It's a professional obligation—and, in a competitive market, a differentiator. Choose tools designed for security from the ground up, not as an afterthought.

Your clients trust you with their most sensitive information. Make sure that trust is well placed.

TheFormTool® is the only major document automation provider that operates entirely offline, with no internet connection required and no background communication of any kind. This guarantees that client data never leaves your system.

See ABA Rule 1.6

Learn more about security

Learn more about Doxserá

Learn more about TheFormTool PRO

TheFormTool LLC

www.theformtool.com

info@theformtool.com