ALM | LAW.COM

New York Law Journal

Invasion of the AI Data Brokers: Advising Clients How to Fight Back

By Douglas Nadjari, Joel Cohen and Yaacov Heidingsfeld
June 4, 2026

The president is currently weighing an executive order to create guardrails against cyberattacks. And recently the pope warned that artificial intelligence can erode the values on which civilized society depends. Both concerns are well-founded—national security, and human dignity. Increasingly, they converge as data collection and surveillance operate on an epic scale.

The rest of us, though, must deal with more individualistic issues and concerns that involve potential problems that may result from AI advancements. As lawyers or law firms in particular that represent clients we have an affirmative duty to ensure that both we and our clients take all the necessary measures to limit the possibility that not only that the client's attorney-client and work product privileges are protected, but that the clients' privacy interests remain secure in general.

And, frankly, in order to know what clients need to know to ensure their privacy or that of their businesses we ourselves, as their lawyers, need to know how to protect our own. Most of us currently simply don't understand AI's capacity to snoop.

Employee Privacy

In 1957, long before modern AI, Vance Packard published "The Hidden Persuaders," a best seller about how advertisers used psychology to shape consumer behavior *generally*. He posed an enduring question: How much manipulation can a free society tolerate before free choice becomes an illusion?

Packard's targets lacked the tools to track a person's movements, habits, speech, health and preferences in real time, then use that data for tailored products, messages and incentives. Today we live in a data economy, and many people still don't grasp how quietly AI systems enter our businesses and private lives, shaping what we, *individually,* see, buy and believe.

It is worth examining how the “big data” industry operates, and what practical steps can reduce digitalprivacy invasion. By clicking “I agree” on terms of use for AI programs, consumers and employees may permit providers to collect prompts, inputs and metadata that reveal private facts, business strategies or privileged material, including attorneyclient or physicianpatient communications. Once disclosed, that information may be retained, analyzed or shared in ways users never anticipated.

Digital voice assistants capture voice data, even when activated inadvertently. Smarthome devices, doorbell cameras and connected televisions log movements, routines and viewing habits, assembling a portrait of daily life.

Wearables do the same with the body. Smartwatches and rings track weight, heart rate, gait, blood pressure, sleep and exercise. According to Ōura Health’s privacy policy, the company processes personal data to provide services, improve products and perform analysis. Users should understand how much continuous biometric information these devices generate—and how sensitive it can be.

Internetenabled cars add another layer. A recent report in the *New York Times* described how software in many vehicles allows manufacturers to collect “telematics”—data on geolocation, latenight driving, speed, lane changes, acceleration and braking. Data brokers then sell this information to auto insurers, which use it to calculate individual rates.

NPR and *Politico* have reported that data aggregators sell personal information to police departments and even the FBI—a profitable practice that allows law enforcement to buy intimate details that until recently would have required a search warrant. The intrusion is deep, but some semblance of privacy may still be salvaged.

Last year California enacted the “Delete Act,” which requires data brokers to register and disclose whether they collect personal information of minors, names, Social Security numbers, birthdates, home. email addresses and phone numbers, connectedtelevision identification numbers, citizenship and immigration status, precise geolocation data, sexual orientation, and reproductivehealth data.

The law also requires disclosure of whether an entity has sold data to any government agency or foreign actor. In its first year, five Californiaregistered brokers reported collecting geolocation data, and 33 disclosed selling or sharing it with actors in North Korea, China, Russia or Iran.

Those are important steps, but only a start. What can individuals and businesses do now?

1. Avoid unnecessary alwayson devices. Don’t use digital voice assistants if you don’t need them, and consider opting out of your auto manufacturer’s connectivity app. The most secure data is the data never collected.

2. Read—or have AI summarize—terms and conditions. If reviewing them yourself seems daunting, turn the technology back on itself: paste the terms into your preferred AI tool and ask for a concise summary of datacollection and sharing practices.

3. If you are a California resident, enroll in the Delete Act program. Exercising your right to demand deletion or restriction of your data not only protects you but signals that these rights will be used.

4. Be extremely cautious with open AI systems. Popular generativeAI tools operate as

"open" systems, and depending on configuration you may be surrendering privacy, sharing proprietary information or jeopardizing attorneyclient privilege. Prefer vetted "closed" systems with strong contractual and technical safeguards, including bans on training models on your data and meaningful audit rights.

5. Businesses must police their own data hygiene. Owners and advisers should review policies and systems to ensure employees—especially those using personal devices—don't share privileged or proprietary information through generativeAI tools. Confidential information should be governed by clear internal rules on what may, and may not, be entered into such systems.

6. Adopt a Know Your Data Broker, or "KYDB," rule. If your client's business is datadriven and you purchase aggregated data, understand where it comes from, how consent was obtained and what contractual limits apply. Demand transparency and document it. Ask whether any data originates from sensitive sources—medical, biometric, geolocation or children's data—and whether it has been sold to foreign or governmental entities.

7. Treat international travel as a special risk. Abroad, your data may be quietly captured by foreign companies or governments under weaker privacy regimes. At the border, U.S. Customs and Border Protection agents are authorized to search personal computers, tablets, phones, flash drives and smartwatches without a warrant. The best practice is to travel with a separate "clean" device and minimize sensitive data stored locally.

AI and datadriven business models are not going away. The urgent task is to insist on meaningful guardrails while taking sensible steps now to limit what can be collected, sold and used against us. Privacy will always carry a cost. The real question is whether we understand the price before we willingly pay it.

Some clients, particularly those who aren't tech-savvy, may be resistant to learning about and implementing some of the more imposing measures outlined above. It's up to us to explain to them the potential dangers that may lurk if they choose aloofness over caution.

Douglas Nadjari, *a former state prosecutor, practices white-collar criminal defense and health care law, is a partner at Ruskin Moscou Faltischek, P.C. He is a member of the Tulane University Law School Criminal Law Boot Camp faculty.* **Joel Cohen***, a former state and federal prosecutor, practices white collar defense law at the Ruskin firm. He is an adjunct professor at both Fordham and Cardozo Law Schools and comments on the law, professional responsibility and social policy for a number of publications.* **Yaacov Heidingsfeld** *is the founder of John Galt Investments LLC. A fintech entrepreneur with three decades of experience, he advises companies on technological disruptions, electronic trading infrastructure, and compliance issues.*