The Computer & Internet Lawyer

Volume 43 ▲ Number 6 ▲ June 2026

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

No Privacy Interest in Internet Searches

By Stephen J. McConnell

Our favorite aspect of being a prosecutor was the investigation phase. Snooping is fun. Figuring out what the crook did and how he did it made us feel like Columbo or Mannix. (Surely those references are lost on anyone under 50. Maybe we should have alluded to Poker Face.) Surveillance, telephone records, and bank accounts often told quite a revealing story. Once we had the evidence, proving it up was relatively easy. There is a reason why most criminal defendants plead guilty. There is a reason why fewer than 1% of federal criminal defendants get acquitted.

By contrast, our least favorite aspect of civil litigation is discovery. It is asymmetrical, burdensome, and expensive. Answering interrogatories, producing millions of pages, and squabbling over privilege logs are time-consuming and soul-destroying activities. There might be some important moments in the course of defending sixty company witness depositions, but what that drudgery mostly produces are transcript pages devoid of significance. It's been said that death is easy, while comedy is hard. For us, trials are easy, while discovery is hard.

The author, a partner in the Philadelphia office of Reed Smith LLP, may be contacted at smcconnell@reedsmith.com.

THE CASE

Commonwealth of Pennsylvania v. Kurtz[1] is a criminal case that has implications for civil discovery. Yes, with that case name, we were tempted to repeat that famous line from Conrad's Heart of Darkness ("The horror, the horror!") (oops – looks like we succumbed to that temptation) — but from our perspective (a former Assistant U.S. Attorney who now defends companies that make fine products), the *Kurtz* case harbors no horrors. In fact, it is interesting, it is insightful, it is correct, and it might even be useful.

Why is that? A defendant in prescription medical product liability litigation could find a plaintiff's internet search history useful for any number of reasons. For example, an internet search history could establish when a plaintiff knew enough to end the discovery rule's tolling of the statute of limitations. It could verify or debunk a plaintiff's claim of being misled by something on the defendant's website. We remember a Baycol case in which a plaintiff claimed that the medicine caused her to suffer rhabdomyolysis, which, she said, made it hard for her to move at all. Then we found a Facebook post where she bragged about recently winning a rodeo barrel race. Good times. Howdy, dismissal.

But discoverability of social media is a snap. It is well established.[2] Can a defendant discover a plaintiff's history from the internet service provider (ISP), or from the search engine? Expect a plaintiff to oppose such discovery, claiming some sort of privacy interest.

But if the litigation is in our home jurisdiction of Pennsylvania, then the *Kurtz* decision, an affirmance by the Pennsylvania Supreme Court in a criminal case, should defeat the plaintiff's privacy claim. That's why we are bloviating about *Kurtz* here. It is an interesting case in its own right. To be sure, it concerns a horrific crime. Kurtz had been convicted of numerous offenses, including rape and kidnapping (involving five victims). Someone invaded a victim's home, kidnapped her, and then raped her. How was the villain caught? The Pennsylvania law enforcement folks did some excellent sleuthing. From the facts of the crime, they deduced that the criminal knew details about the victim's home and habits. The police obtained a "reverse keyword search warrant" for the records that Google generated during the week prior to the assault. The warrant was not directed at a specific person's activity, but instead targeted all searches performed on Google's search engine relating to the victim's name and address. Voila — the defendant had performed two such searches in the hours before the crime.

ISP/SEARCH ENGINE SEARCHES

By the way, expect to see more of this sort of use of ISP/search engine searches. Surely, you've heard of cases in which a murder defendant ran searches on not-very-innocent topics. The slayer of Idaho college students had conducted internet searches on "rape," "voyeur," "forced," and "sleeping." Convicted murderer Brian Walshe used Google to look up ways to dismember and dispose of a body. (Luckily for us, our own internet searches are on dull topics such as "Why won't my sourdough starter start?" or "parking spots for fishing in Pickering Creek." You will not find inquiries about "best stabbing knives" or "how to make poisoned tiramisu.")

It turned out that defendant Kurtz was a correctional officer who worked with the victim's husband. The police obtained a DNA sample from the defendant (via a discarded cigarette butt), there was a match, there was an arrest, and then the defendant confessed to the rape (and four others). That is a pretty solid criminal case. Nevertheless, the defendant filed a motion to suppress the Google search (and all fruits of that allegedly poisonous tree). He lost that motion, then proceeded to trial. The jury convicted him. Kurtz filed an appeal. The key issue on appeal was whether the Google search violated the defendant's Fourth Amendment right against an unreasonable search and seizure. One unwritten rule in criminal appeals is that Bad Man Stays in Jail. Kurtz's appeal was never going to win. He seems an utter scoundrel. But at least he raised an issue that made good law for those of us who are Not a Bad Man.

THE COURT'S DECISION

The Pennsylvania Supreme Court majority held in *Kurtz* that people who search the internet voluntarily provide that data to a third party, the search engine, and thus have no reasonable expectation of privacy in their Internet searches. (Justice Mundy authored a concurrence. Only one Justice, Donohue, thought the defendant had a reasonable expectation of privacy in the Google searches.) The absence of a reasonable expectation of privacy means that there was no "search" under the Fourth Amendment. The "third party" doctrine holds that, generally, a person lacks an expectation of privacy under the Fourth Amendment in information or materials when that person exposes them to a third party. (We had a jolly time convicting a serial bank robber who had dropped off a bag at his ex-wife's house. The bag contained, among other things, a list of banks robbed and to be robbed. The ex-wife – big surprise – did not like her ex-husband very much. She was delighted to hand the incriminating bag and list over to the FBI.)

The third party doctrine clearly came into play in the *Kurtz* case, as the terms and conditions of the search engine (here, Google) defeat any privacy expectation. The court held that "what matters is that the user is informed that Google—a third party—will collect and store that information. When the user proceeds to conduct searches with that knowledge, he or she voluntarily provides information to a third party. This express warning, in tandem with the more indirect indicators noted above, necessarily precludes a person from claiming an expectation of privacy in his or her voluntary internet use."

Thus, as alluded to above, Bad Man Stays in Jail. And maybe, if you manage to do some of your own sleuthing, Phony Plaintiff Gets Skunked.

Notes

1. Commonwealth of Pennsylvania v. Kurtz, 2025 WL 3670767 (PA Dec. 16, 2025).
2. See https://www.druganddevicelawblog.com/2011/11/e-discovery-for-defendants-cheat-shee.html.