Pennsylvania Supreme Court Holds No Reasonable Expectation of Privacy in Internet Search Activity: Key Takeaways for Employers

Insights
1.07.26

A recent Pennsylvania Supreme Court ruling could have broad implications for internet privacy, and employers should take note. The state's high court ruled in December that individuals do not have a reasonable expectation of privacy in their internet search activity for purposes of the Fourth Amendment and similar state constitutional protections. Although the case centered on a state police search in a criminal investigation, the decision will likely influence how courts applying Pennsylvania law analyze privacy expectations across a wide range of contexts, including matters concerning employment and the workplace. This Insight will discuss *Commonwealth v. Kurtz* and how this decision could impact private employers.

Background on *Commonwealth v. Kurtz*

In an investigation into a violent crime, state police obtained a "reverse keyword search warrant" that instructed Google to identify anyone who searched the victim's name or home address in the week before the assault. Google informed the police that someone had searched the victim's address a few hours before the attack, and the investigators used this information (and the IP address used for the searches) to identify, track, obtain DNA evidence, and arrest the suspect, who confessed to the crimes and similar crimes involving four other victims.

When the cases went to trial, the defendant asked the court to suppress the evidence pulled from the police's search of Google's records, challenging the validity of the search warrant used to obtain them. After the trial court denied that request, a jury found Kurtz guilty on all counts, and the state's Superior Court affirmed.

PA Supreme Court: No Enforceable Expectation of Privacy in Most Internet Searches

The Supreme Court of Pennsylvania affirmed on December 16.

- Kurtz argued that the state police violated his Fourth Amendment and state constitutional rights because the police failed to establish probable cause individualized to him when they obtained the search warrant for the Google records.

- However, the court held that the Fourth Amendment was not triggered at all because Kurtz did not have a reasonable expectation of privacy in his unprotected internet searches. It therefore declined to reach the probable cause challenge.

In deciding the case, the state's high court:

- **emphasized that internet users knowingly and voluntarily transmit information to third-party service providers** when they conduct online searches – and therefore cannot reasonably expect that such information will remain private. (In the court's words, although internet users may *believe* their searches are private, "even the ordinary, everyday use of the internet provides strong indicators that there is no privacy in the terms or information that the user voluntarily enters into a search engine.")
- **rejected arguments that the Pennsylvania Constitution provides broader privacy protections for internet search activity** than the federal Constitution, expressly holding that no reasonable expectation of privacy exists under either framework.
- **distinguished internet use from the Fourth Amendment protections granted to cell-site location information** in a 2018 US Supreme Court decision. (The court explained that "the use of the internet is not an inextricable and involuntary aspect of our daily life in the same way that mobile phones have become" and "[t]hat the internet is helpful, readily available, and convenient does not render its use involuntary in such a way that a person today has no choice but to rely upon it and, derivatively, has no choice but to share information with third parties.")

Importantly, however, the Pennsylvania high court limited its decision to "general, unprotected internet use." The court made clear that internet users who take efforts "to secure some degree of privacy" may be afforded greater constitutional privacy protections. The court pointed to use of virtual private networks, internet browsers that do not collect or share data, and websites that are password-protected as examples of internet use that may permit users to "retain a constitutionally recognizable expectation of privacy."

How This Decision Could Impact the Workplace

Constitutional bans (whether state or federal) on unreasonable searches and seizures do not apply at all to purely private conduct. A private employer that is not acting as an agent of the government cannot violate an employee's constitutional privacy protections – though many other privacy laws and concerns must be considered. Although the *Commonwealth v. Kurtz* ruling directly addressed law enforcement's access to internet search information during criminal investigations, its practical implications could be far-reaching:

- **Workplace Investigations:** Internet searches and browsing history often are probative in workplace investigations of employee conduct, where employers confront questions about employee internet usage, browsing history, and online searches conducted on employer-provided devices or networks. This decision reinforces the principle that such activity lacks a

reasonable expectation of privacy and supports an employer's ability to collect and rely on search data during internal investigations without triggering privacy violations, particularly when coupled with strong acceptable-use and electronic communications policies, as noted below.

- **Electronic Discovery and Litigation:** The court's reasoning may also influence how courts address privacy objections in civil discovery disputes. Litigants frequently resist producing browsing history, search terms, and related metadata because they argue that such information is highly personal or intrusive. However, now that the court has ruled that constitutional privacy protections do not automatically apply to internet search activity, Pennsylvania courts evaluating discovery disputes may be less receptive to objections where parties are found to have shared their search history or browsing data with third-party platforms, provided the requested information is relevant and proportional.
- **Technology and Privacy Policies:** As courts continue to recognize diminished expectations of privacy in online activity, employers should ensure that their acceptable-use and electronic communications policies accurately reflect how workplace technology is used and monitored. Clear policies can help set employee expectations, reduce the risk of privacy-based challenges, and strengthen an employer's position when reviewing internet activity on employer-provided devices and networks in connection with investigations, compliance reviews, or litigation.

Key Takeaways for Employers

- Courts are increasingly skeptical of claims that internet search activity is private.
- The voluntary transmission of data to third parties significantly undermines privacy expectations.
- Employers should ensure their electronic communications and internet-use policies accurately reflect modern privacy realities.
- Even though this was a criminal case, its reasoning is likely to influence civil and employment-related disputes involving digital information.

Conclusion

We will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox. If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Privacy and Cyber Practice Group.

Related People

Risa B. Boerner, CIPP/US, CIPM
Partner
610.230.2132
Email

Catherine M. Contino
Associate
610.230.6109
Email

Jordan A. Jiles
Associate
412.822.6636
Email

Christopher J. Merken
Associate
610.230.6119
Email

Service Focus

Privacy and Cyber

Litigation and Trials

Workplace Investigations

Related Offices

Pittsburgh

Philadelphia