DLG LEARNING CENTER

CIRCUIT COURTS OF APPEAL · FOURTH AMENDMENT · LEGAL UPDATE · RESOURCES

Bytes and Bounds: Holcomb's Warning Against Unfettered Electronic Searches

By **Daigle Law Group**

July 24, 2025

DAIGLE LAW GROUP

dlglearningcenter.com

Bytes and Bounds: Holcomb’s Warning Against Unfettered Electronic Searches

By Daigle Law Group · July 24, 2025

The United States Court of Appeals for the Ninth Circuit issued a decision in United States v. Holcomb, 23-469 (9th Cir. 2025), where the Court considered “whether an individual can be prosecuted for despicable criminal conduct based on evidence obtained in violation of the United States Constitution. Ultimately, the Circuit wrote, “In the circumstances of this case, respect for the Constitution and the rule of law requires an answer of “no.”

Factual Summary

On January 28, 2020, officers with the Burlington Police Department responded to a 911 call at the home of John Holcomb. Officers arrived at the residence and received troubling information from Holcomb himself. Holcomb informed the officers that he had recently rescued his ex-girlfriend “J.J.” from sex slavery, that she had started acting crazy, and he wanted her to leave. When the police spoke with J.J., she told them she had been sexually assaulted by Holcomb and that he had filmed the assault. Hoping to clear his name, Holcomb provided officers with his password for his computer and gave consent for them to watch the video of what he characterized as a consensual sexual encounter. Eventually, Holcomb revoked consent before the point at which law enforcement actually viewed the footage. Later that day, Holcomb was arrested based on allegations of rape and law enforcement obtained a warrant which authorized the seizure, but not the search, of Holcomb’s computer and cell phone. On February 4th, 2020, police obtained a search warrant for the search of the computer, categorized into five areas of evidence. Four of these categories were limited to date ranges between June of 2019 and the dates surrounding the incident, and sought videos, images, communications, and other data related to the alleged rape. The fifth category of evidence sought was data which would demonstrate “dominion and control” over the device, though this category was not limited to any particular period or specific type of file. During the search of the computer by a forensic examiner, video of the alleged incident was recovered which seemed to corroborate Holcomb’s account. However, the examiner continued to search the computer by scrolling through files and observed that several of the thumbnails seemed to depict child pornography. When the examiner opened the thumbnails, the videos appeared to be recordings of Holcomb sexually assaulting his underaged daughter, along with other images of underaged persons in various stages of undress. All of the latter videos and photos were dated from 2016.

Procedural Posture

While the sexual assault case was dismissed, the child pornography case was referred to FBI and Holcomb was ultimately indicted by a federal grand jury on one count of producing child pornography in violation of 18 U.S.C. § 2251(a). At the district court, the defendant once again filed a motion to suppress the evidence of the three videos, arguing that the warrant authorizing the search was overbroad and not sufficiently particularized to comply with the Fourth Amendment. However, the district court disagreed and denied the motion. The court found that even if the warrant was obtained in violation of his constitutional rights, admissibility was proper because the good faith exception was applicable. The defendant pled guilty to the charges and appealed to the Ninth Circuit. On appeal, the defendant advanced several arguments. First, that the second warrant dominion and control provision, on the basis of which the examiner located the three videos that led to Holcomb's indictment, was invalid because it was both overbroad and insufficiently particular. He further argues that, under Ninth Circuit precedent, the good-faith exception does not apply to the examiner's search of his computer. In response, the government challenges each of these arguments and also argues that the plain view doctrine independently authorized the examiner's seizure of the three videos depicting child sexual abuse.

United States Court of Appeal for the Ninth Circuit

When the case reached the Ninth circuit, the court reversed the lower court's ruling on Holcomb's motion to suppress, vacated his conviction, and remanded the case. The Court made three key holdings; first, that the dominion and control provision was invalid because it was both overbroad and insufficiently particular; Second, that the good-faith exception does not apply to the examiner's search; and finally, that the plain view doctrine does not independently justify the examiner's seizure of the videos. The Ninth Circuit Court of Appeals first addressed the issue of whether the warrant amounted to what may be described as an unconstitutional "general warrant." Here, Officers were authorized to search the entire contents of Holcomb's computer, with no time limits on the files they could review. The Court explained that 'Dominion and control' over the device were never in dispute—Holcomb freely gave his passwords and walked investigators through how to access his system. Yet by granting unlimited discretion to sift through every folder and document, the warrant crossed the line into a general "rummaging" authority, which contravenes the Fourth Amendment. The court made clear that, although date restrictions and temporal limits aren't mandatory in every digital search, the government must tailor its requests when specificity is both feasible and constitutionally required, as it should have done here.

Next, the court tackled the issue of whether the evidence was admissible based on the good faith exception to the Exclusionary Rule. Under the good faith exception, officers relying objectively and reasonably on a warrant later invalidated can still satisfy the Fourth Amendment. Here, the government argued for admissibility on qualified immunity grounds—essentially that the law wasn't yet "clearly established" against blanket digital searches. The Ninth Circuit disagreed: longstanding precedents had already warned that warrants lacking both precise evidentiary restrictions and temporal boundaries run afoul of the Constitution. Because a reasonable officer in 2019 would have known that authorizing a blanket search for evidence of "dominion and control" without further justification violates the Fourth Amendment, the good-faith exception did not apply. To advance its reasoning, the court cited several cases where law enforcement failed to include the type of evidence sought or to provide temporal limitations for the search, which had been previously established as violating the Fourth Amendment. Based on these findings, the court found that the evidence did not meet the good faith exception since the law was clearly established. Finally, the court rejected the government's fallback reliance on the Plain View Doctrine for admissibility of the evidence. Although the examiner stumbled upon these explicit thumbnails during the search executed under the warrant, those discoveries derived directly from a warrant the court deemed overly broad and invalid. The court concluded that because the warrant fell into the category of unconstitutional general warrants, any resulting discoveries were invalid and inadmissible.

Key Takeaways

For law enforcement, remember that the digital realm of evidence must be approached using the same principles applicable to acquiring physical evidence. Warrants must target and limit the search to where and when you expect to find evidence. If you know a crime took place on a particular date, your warrant should identify a reasonable time window around that incident—say, files created or accessed in the days immediately before or after—and specify the kinds of data you're seeking. Simply authorizing officers to sift through an entire device without temporal or categorical limits turns a lawful search into an unconstitutional "general warrant." By tying your probable cause to a defined period and describing the specific records or file types connected to the investigation, you honor the Fourth Amendment's requirement of particularity and strengthen the foundation for any evidence you recover.

United States v. Holcomb, 23-469 (9th Cir. 2025)