EFF to Tenth Circuit: Protest-Related Arrests Do Not Justify Dragnet Device and Digital Data Searches

Brendan Gilligan, Saira Hussain, and Jennifer Lynch ⋮ 6-7 minutes ⋮ 9/3/2024

The Constitution prohibits dragnet device searches, especially when those searches are designed to uncover political speech, EFF explained in a friend-of-the-court brief filed in the U.S. Court of Appeals for the Tenth Circuit.

The case, *Armendariz v. City of Colorado Springs*, challenges device and data seizures and searches conducted by the Colorado Springs police after a 2021 housing rights march that the police deemed "illegal." The plaintiffs in the case, Jacqueline Armendariz and a local organization called the Chinook Center, argue these searches violated their civil rights.

The case details repeated actions by the police to target and try to intimidate plaintiffs and other local civil rights activists solely for their political speech. After the 2021 march, police arrested several protesters, including Ms. Armendariz. Police alleged Ms. Armendariz "threw" her bike at an officer as he was running, and despite that the bike never touched the officer, police charged her with attempted simple assault. Police then used that charge to support warrants to seize and search six of her electronic devices—including several phones and laptops. The search warrant authorized police to comb through these devices for all photos, videos, messages, emails, and location data sent or received over a two-month period and to conduct a time-unlimited search of 26 keywords—including for terms as broad and sweeping as "officer," "housing," "human," "right," "celebration," "protest," and several common names. Separately, police obtained a warrant to search all of the Chinook Center's Facebook information and private messages sent and received by the organization for a week, even though the Center was not accused of any crime.

After Ms. Armendariz and the Chinook Center filed their civil rights suit, represented by the ACLU of Colorado, the defendants filed a motion to dismiss the case, arguing the searches were justified and, in any case, officers were entitled to qualified immunity. The district court agreed and dismissed the case. Ms. Armendariz and the Center appealed to the Tenth Circuit.

As explained in our amicus brief—which was joined by the Center for Democracy & Technology, the Electronic Privacy Information Center, and the Knight First Amendment Institute at Columbia University—the devices searched contain a wealth of personal information. For that reason, and especially where, as here, political speech is implicated, it is imperative that warrants comply with the Fourth Amendment.

The U.S. Supreme Court recognized in *Riley v. California* that electronic devices such as smartphones "differ in both a quantitative and a qualitative sense" from other objects. Our electronic devices' immense storage capacities means that just one type of data can reveal more than previously possible because they can span years' worth of information. For example, location data can reveal a person's "familial, political, professional, religious, and sexual associations." And combined with all of the other available data—including photos, video, and communications—a device such as a smartphone or laptop can store a "digital record of nearly every aspect" of a person's life, "from the mundane to the intimate." Social media data can also reveal sensitive, private information, especially with respect to users' private messages.

It's because our devices and the data they contain can be so revealing that warrants for this information must rigorously adhere to the Fourth Amendment's requirements of probable cause and particularity.

Those requirements weren't met here. The police's warrants failed to establish probable cause that any evidence of the crime they charged Ms. Armendariz with—throwing her bike at an officer—would be found on her devices. And the search warrant, which allowed officers to rifle through months of her

private records, was so overbroad and lacking in particularity as to constitute an unconstitutional “general warrant.” Similarly, the warrant for the Chinook Center’s Facebook messages lacked probable cause and was especially invasive given that access to these messages may well have allowed police to map activists who communicated with the Center and about social and political advocacy.

The warrants in this case were especially egregious because they appear designed to uncover First Amendment-protected activity. Where speech is targeted, the Supreme Court has recognized that it’s all the more crucial that warrants apply the Fourth Amendment’s requirements with “scrupulous exactitude” to limit an officer’s discretion in conducting a search. But that failed to happen here, and thus affected several of Ms. Armendariz and the Chinook Center’s First Amendment rights—including the right to free speech, the right to free association, and the right to receive information.

Warrants that fail to meet the Fourth Amendment’s requirements disproportionately burden disfavored groups. In fact, the Framers adopted the Fourth Amendment to prevent the “use of general warrants as instruments of oppression”—but as legal scholars have noted, law enforcement routinely uses low-level, highly discretionary criminal offenses to impose order on protests. Once arrests are made, they are often later dropped or dismissed—but the damage is done, because protesters are off the streets, and many may be chilled from returning. Protesters undoubtedly will be further chilled if an arrest for a low-level offense then allows police to rifle through their devices and digital data, as happened in this case.

The Tenth Circuit should let this case to proceed. Allowing police to conduct a virtual fishing expedition of a protester’s devices, especially when justification for that search is an arrest for a crime that has no digital nexus, contravenes the Fourth Amendment’s purposes and chills speech. It is unconstitutional and should not be tolerated.

Join EFF Lists