People v. Wilson

(2020) __ Cal.App.5th __ [2020 WL 6153696]

Issues

(1) Did a routine search of emailed photos by Google constitute a "police" search? (2) When these photos were transmitted to a law enforcement task force, were officers required to obtain a warrant before viewing them?

Facts

Whenever a photo is attached to an email sent via Google, an algorithm automatically scans it for indications that it contains child pornography. This is accomplished by comparing the photo with photos that are stored in a repository of child pornography. This comparison is conducted by the algorithm which examines the features of the photo and converts them into an alphanumeric "hash value." It then compares that hash value with the hash values of photos that are stored in a repository of photos in a child pornography repository on file that have been identified as child pornography. If there is a sufficient match, Google will transmit an alert or "Cybertip" to the National Center for Missing and Exploited Children (NCMEC). The Cybertip will include a copy of the photos.

When it receives a Cybertip, NCMEC will do one of two things: (1) physically open the photos to determine whether they do, in fact, constitute child pornography, or (2) send the photos to the law enforcement agency that has jurisdiction in the matter.

In *Wilson*, Google's computer flagged four photos that had been attached to an email that was sent or received by Luke Wilson in San Diego. Accordingly, the letters were transmitted to NCMEC which, without reviewing them, transmitted them to the San Diego Internet Crimes Against Children task force (ICAC) which is run by state and federal law enforcement officers. ICAC investigators then opened the files and confirmed that they constituted child pornography. The investigators then obtained a warrant to search Wilson's "apartment and vehicle, and to seize computer equipment, storage devices, and other effects." During the search, officers found the four photos and much more. Furthermore, based on information included in Wilson's emails, were able to identify the children in the photos. As the result, Wilson was charged with one count of oral copulation of a child 10 years or younger, and three counts of committing a lewd act upon a child.[1] His motion to suppress the photos was denied and, following a jury trial, he was convicted and sentenced to a prison term of 45 years to life.

Discussion

Wilson argued that his motion to suppress should have been granted for two reasons: (1) Google functions as a law enforcement agency when it scans email attachments for child pornography and, therefore, a warrant was required. (2) ICAC agents needed a warrant to open the files.

"Police" vs. "private" searches

A search conducted by a person who is neither a law enforcement officer nor a police agent is not a search covered by the Fourth Amendment and, therefore, a warrant is not

[1] Pen. Code §§ 288.7, 288(a).

required.[2] To determine whether a search was private, the test is whether an officer played such a role in the person's decision to search, or in his decisions on how and where to search, that the intrusion can fairly be attributed to the officer; i.e., everything depends on "the degree of the Government's participation in the private party's activities."[3]

Consequently, a person will be deemed a police agent if an officer requested, encouraged, assisted, or authorized the person to conduct the search.[4] In other words, a police search will result if there was "some evidence of Government participation in or affirmative encouragement." In *Wilson*, it was apparent that no government agency was involved in Google's routine practice of scanning email attachments to determine if they contain child pornography. In the words of the court:

> All of Google's actions—including scanning user content, assigning hash values to that content, comparing user content to a repository of hash values, flagging offending images with hash values that match previously-reviewed child pornography images, and sending the apparent child pornography to NCMEC—constitute private action that was not performed at the direction of the government.

Did NCMEC or ICAC agents need a warrant?

Officers who receive computer files that were obtained in the course of a private search may open them without a warrant only if, by doing so, they did not see anything that the sender had not already seen. (This rule also applies to unopened containers that officers receive from a citizen.[5]) The theory here is that people cannot reasonably expect privacy as to photos or information that had already been lawfully examined by the people who provided them to officers. As the Supreme Court explained, "Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information."[6]

Consequently, Wilson argued that he retained a reasonable expectation of privacy in the photos because no employee of Google or NCMEC had actually seen them, and he

---

[2] See *US v. Jacobsen* (1984) 466 US 109, 113 ["[The Fourth Amendment] is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official."]; *Skinner v. Railway Labor Exec. Assn.* (1989) 489 US 602, 614 [evidence will be suppressed if it was obtained as the result of an unlawful search by civilian who was an "instrument or agent of the Government"].

[3] *Skinner v. Railway Labor Exec. Assn.* (1989) 489 US 602, 614. **USSC**: *Lustig v. US* (1949) 338 US 74, 78 [did the officer "have a hand" in the search?].

[4] See *Lugar v. Edmondson Oil Co.* (1982) 457 US 922, 941 ["a private party's joint participation with state officials in the seizure of disputed property is sufficient to characterize that party as a 'state actor'"]; *US v. Jacobsen* (1984) 466 US 109, 113 [search "with the participation" of an officer];"].

[5] See, for example, *US v. Jacobsen* (1984) 466 US 109, 115 ["Whether [the initial opening of the package by Federal Express employees was] accidental or deliberate, and whether [it was] reasonable or unreasonable, [it] did not violate the Fourth Amendment because of their private character."]. **CAL**: *Miramontes v. Superior Court* (1972) 25 CA3 877, 884 [when airline employees discovered marijuana in a package, it was reasonable for them "to call on the police for expert assistance."];

[6] *US v. Jacobsen* (1984) 466 US 109, 117.

still had a reasonable expectation of privacy in their contents. Instead, as noted, this determination was based on a match between the hash values of the photos and stored photos that had been determined to constitute child pornography.

This was true, said the court, but any privacy expectation that Wilson might have had as to the contents of the photos was eliminated when two things occurred: (1) Google's algorithms searched them and identified features that were identical to child pornography in its repository, and (2) all of the photos that had been added to the repository had been examined by a Google employee who confirmed that they constituted child pornography. As the court explained:

> The government was merely reviewing what Google had already found, but in a different format—visually reviewing the photographs with the agent's human eye versus replicating the computer's generation of a numerical algorithm. Because the assigned numerical values, or "digital fingerprints," are representative of the contents depicted in the photographs themselves, the government gained no ne material information by viewing the images.

Accordingly, the court ruled that the officers did not conduct a "search" when they viewed the photos, and it affirmed Wilson's conviction. POV

Date posted: