STATE OF MINNESOTA
IN COURT OF APPEALS
A12-1206

State of Minnesota,
Respondent,

vs.

Patrick Michael VanLandschoot,
Appellant.

Filed April 8, 2013
Affirmed
Peterson, Judge

Washington County District Court
File No. 82-CR-11-193

Lori Swanson, Attorney General, St. Paul, Minnesota; and

Peter James Orput, Washington County Attorney, Jessica Lynn Stott, Assistant County Attorney, Stillwater, Minnesota (for respondent)

Michelle Margoles, Alan D. Margoles, St. Paul, Minnesota (for appellant)

Considered and decided by Peterson, Presiding Judge; Ross, Judge; and Chutich, Judge.

U N P U B L I S H E D O P I N I O N

PETERSON, Judge

In this appeal from his conviction of possession of a pornographic image involving minors, appellant argues that the district court erred by refusing to suppress evidence discovered pursuant to an administrative subpoena. Because appellant failed to meet his

burden of showing that he had a legitimate expectation of privacy in the seized evidence, we affirm.

FACTS

Minneapolis police officer Dale Hanson, a member of the Internet Crime Against Children Task Force (ICAC), investigates internet child-pornography distribution. Hanson uses two software programs to screen internet postings for certain "hash values" that indicate probable child pornography. This software focuses on peer-to-peer networks that permit users to publicly share images. Hanson ran these two software programs on August 13 and 16, 2010. One software program identified a particular internet protocol (IP) address as containing suspected child-pornography files. Hanson was able to download files from this IP address and visually examine them; he concluded that at least four of the files contained child-pornography images. The IP address used LimeWire, a peer-to-peer network that permits users to search public networks for downloadable files and enables users' files to be publicly downloaded.

With the same software, Hanson obtained an approximate geographic location for the IP address, which was in St. Paul, and identified Comcast as the internet service provider associated with the IP address. Using this information, Hanson submitted a form application for an administrative subpoena pursuant to Minn. Stat. § 388.23 (2010), to the Hennepin County Attorney's Office, the county attorney for Hanson's jurisdiction as a Minneapolis police officer. The administrative-subpoena application form is a standard form; Hanson identified the records requested, checked a line specifying "Type of Business," certified that the information was needed for "an ongoing, legitimate law

enforcement investigation of Distribution of Child Pornography," and signed the form. An assistant Hennepin County attorney signed the subpoena form on August 17, 2010. A few days later, Hanson received information from Comcast that identified appellant Patrick Michael VanLandschoot's mother, P.V., as the person associated with the IP address. Comcast also provided P.V.'s home address in Cottage Grove in Washington County, her telephone number, her account number and the type of service she received, her method of payment, and the e-mail "User Ids" associated with her account. Hanson forwarded the information to another ICAC task force member at the Woodbury Police Department, who contacted an investigator at the Cottage Grove Police Department. After reviewing these materials, the investigator applied for and received a judicially issued warrant to search P.V.'s house. The investigator interviewed appellant, who admitted that he downloaded the materials and that the files were on a computer in an upstairs bedroom.

Appellant was charged with one count of possession of a pornographic image involving minors, in violation of Minn. Stat. § 617.247, subd. 4(a) (2010). Following a contested omnibus hearing, the district court refused to suppress evidence recovered as the result of the administrative subpoena. Appellant agreed to a trial on stipulated evidence while preserving the right to appeal pretrial issues, pursuant to Minn. R. Crim. P. 26.01, subd. 4. The district court found appellant guilty, stayed imposition of sentence for five years, and placed appellant on probation. Appellant challenges the district court's refusal to suppress the evidence provided by Comcast pursuant to the administrative subpoena.

D E C I S I O N

Appellant argues that use of the statutory administrative-subpoena process allowed an unconstitutional search and seizure under the federal and the state constitutions because the statute "does not provide for any review by a judicial magistrate or any finding of cause, much less probable cause." Appellant also argues that the administrative-subpoena process denied "all due process of the law, because individuals are given no opportunity to be heard before their privacy rights have been intruded upon." Appellant contends that searches "outside of the judicial warrant process are per se unreasonable" and he had a "reasonable expectation of privacy in the information seized." Therefore, appellant concludes, all evidence seized as a result of the administrative subpoena must be suppressed.

"Minnesota statutes are presumed to be constitutional, and the power to declare a statute unconstitutional is exercised with extreme caution and only when absolutely necessary." *Greene v. Comm'r of Minn. Dept. of Human Servs.*, 733 N.W.2d 490, 494 (Minn. Ct. App. 2007) (quotation omitted), *aff'd*, 755 N.W.2d 713 (Minn. 2008). We review de novo a challenge to a statute's constitutionality. *Hamilton v. Comm'r of Pub. Safety*, 600 N.W.2d 720, 722 (Minn. 1999).

Both of the constitutional challenges that appellant raises rest on the premise that use of the administrative-subpoena process resulted in the denial of appellant's constitutional right to be free from an unreasonable search and seizure. *See* U.S. Const. amend. IV ("right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated"); Minn. Const. art. I,

§ 10 ("right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated"). Appellant has the burden of establishing that use of the administrative subpoena violated his rights under the Fourth Amendment to the United States Constitution and Article I, § 10, of the Minnesota Constitution by infringing on a protected privacy interest. *State v. Gail*, 713 N.W.2d 851, 859 (Minn. 2006). "[T]here is no standing to raise a constitutional challenge absent a direct and personal harm resulting from the alleged denial of constitutional rights." *City of Minneapolis v. Wurtele*, 291 N.W.2d 386, 393 (Minn. 1980).

The constitutional protections against unreasonable searches and seizures are not triggered unless a person has a legitimate expectation of privacy. *Gail*, 713 N.W.2d at 860. In *Gail*, the Minnesota Supreme Court described the two-step analysis used to determine whether a protected privacy interest was infringed when an administrative subpoena was used to obtain cell-phone records from Verizon Wireless: the first step was to determine whether Gail exhibited an actual subjective expectation of privacy in the records; the second step was to determine whether that expectation of privacy was reasonable. *Id.* at 860. The supreme court explained that, in the first step, courts should examine the individual's conduct and determine whether the individual sought to preserve something as private. *Id.* The supreme court concluded that Gail, who "leased" a cell phone from a person who had "leased" it from another person who had a cell-phone contract with Verizon, was a "stranger" to Verizon, the holder of the subpoenaed records, and, as such, Gail could not "subjectively expect[] Verizon to keep records of his cell phone usage private." *Id.*

Here, the district court concluded that appellant did not demonstrate a subjective expectation of privacy in the Comcast records because appellant was not the account holder, did not pay the Comcast bills, did not attempt to conceal his activities, and had not asked Comcast to conceal his identity. We agree. Appellant was a "stranger" to Comcast, and, on this record, he failed to meet his burden of establishing that he had a subjective expectation of privacy in the Comcast records.

Even if appellant were able to claim a subjective expectation of privacy in the records, he cannot demonstrate a reasonable expectation of privacy. In *United States v. Miller*, 425 U.S. 435, 442, 96 S. Ct. 1619, 1623 (1976), the Supreme Court noted that a person has no legitimate expectation of privacy in information that he has provided to a third party, "knowingly" exposing it to the public. The Supreme Court concluded that a person had no privacy interest in bank records because the records "contain[ed] only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." 425 U.S. at 442, 96 S. Ct. at 1624. The Supreme Court explained:

> This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by [the third party] to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

Id. at 443, 96 S. Ct. 1624.

Because we conclude that appellant failed to meet his burden of establishing that use of the administrative subpoena violated his rights by infringing on a protected privacy

interest, we do not reach his objections to procedural defects in the use of the administrative-subpoena process. *See Gail*, 713 N.W.2d at 861 (declining to examine claims of procedural defects in administrative subpoena when objecting party has no subjective privacy expectation).

Affirmed.