VLCT NEWS REPRINT
Serving and Strengthening Vermont Local Governments

Search Warrants in the Digital Age

Technology moves fast. The law, however, does not. In what can be best be characterized as a classic tortoise-hare relationship, the law woefully lags behind in resolving legal questions raised by technologically driven changes to our daily lives. In spite of the ubiquitous nature of computing devices, the recently decided case of *In re Application for Search Warrant*, 2012 VT 102 represents the Vermont Supreme Court's first balancing of the privacy concerns with the ability of law enforcement to conduct effective criminal investigations against the backdrop of the unique challenges posed by the digital world.

The Fourth Amendment to the U.S. Constitution and its Vermont corollary, Chapter I, Article 11, protect our reasonable expectations of privacy against governmental intrusion. These privacy rights are safeguarded by judicial officers who may grant a warrant "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Constitution, Amend. IV.

Ironically, the facts of this case concern the privacy rights of a person being investigated for allegedly violating those of another by committing the crime of online identity theft. The complaint, originating in New York, was transferred to the Burlington Police Department after a bank involved revealed that the information contained on its credit card application listed an incorrect physical address in Burlington. The Burlington detective assigned to the case applied for a warrant to search the premises at 145 Pleasant Avenue for evidence of the crime of identity theft including permission to seize records regardless of ownership and format, such as those that may be located in any electronic devices. In response to the very broad scope of the warrant application, the judicial officer attached several conditions including restricting investigators' reliance upon the "plain view doctrine" as a basis for seizing any incriminating evidence unrelated to alleged offense, requiring third parties to conduct the search and limiting what methods and instruments could be utilized in executing it, prohibiting the transfer of any evidence unrelated to the suspected offense to state agents, segregating and redacting non-evidentiary data from that dealing with identity theft, and prohibiting those conducting the search from disclosing their work to prosecutors and investigators. Collectively, these conditions on warrants and how they are executed are referred to as *ex ante* conditions, meaning they are imposed before the search is actually conducted. The State opposed their imposition in a motion for extraordinary relief to the Vermont Supreme Court on the grounds that the judicial officer lacked the authority to impose such conditions, and that they were unnecessary and served only to frustrate their criminal investigation.

Justice Dooley, writing for the majority, saw two searches being conducted. The first was for the computer itself: to search the premises and take the computer. That search wasn't in question. The second was for a search of the contents of the computer, a search that raised several issues for the Court to resolve. The first issue of interest to municipalities was the general question of whether a judicial officer can attach prospective conditions on how such a search is to be performed to protect the privacy interests of the person to be searched. That question was one of first impression for the Court as typically these questions are raised in the context of whether evidence already seized can be used against a defendant. If so, then the second question became whether the imposition of the particular conditions in this case constituted an abuse in the exercise of judicial discretion.

To the first point, the State argued that judicial officers are limited when issuing warrants to deciding whether probable cause (reasonable grounds to suspect a crime has been committed) exists and whether the warrant application sufficiently describes the place to be searched and the things to be seized (i.e., "particularity"). Any attempt to direct the manner in which searches are to be executed is beyond the reach of the Court and a clear abuse of power. Unconvinced, the Court could find no such "bright line" establishing a blanket prohibition on *ex ante* instructions. On the contrary, the Court reasoned, Vermont law hints at its past use. These instructions have also been used in more traditional contexts to ensure particularity by limiting the scope of searches to a particular room and not an entire house or instructing how to locate the items to be seized. "In other words, some *ex ante* constraint – of the form 'here, not there' – are perfectly acceptable." These types of instruction, the Court reasoned, have great relevance and applicability to the difficulties of the digital world "where physical notions of particularity are metaphorical at best. ... The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important."

Having accepted the practice of levying digital *ex ante* instructions in general, the Court next turned its attention to whether the specific instructions given in this case constituted an abuse of authority. Here we'll focus on those instructions of note. The first instruction related to the plain view doctrine, which the U.S. Supreme Court described thusly: "If police are lawfully in a position from which they view an object, if its incriminating character is immediately apparent, and if officers have a lawful right of access to the object, they may seize it without a warrant." *Minnesota v. Dickerson*, 508 U.S. 366, 375 (1993). The judicial officer granting the warrant in this case prohibited the State from seizing any electronic records other than those authorized by the warrant as well as its reliance upon the plain view doctrine. The Court, on this point, agreed with the State that the judicial officer overreached by refusing to apply legal principles in certain situations. Allowing this, the Court held, would allow courts to "disregard the considered limitations of the law it is charged with enforcing." The Court also found the instruction unnecessary because other instructions restricting with whom the results could be shared and separating the search from the investigatory functions eliminated the possibility of viewing any incriminating evidence not described in the warrant in the first place.

The Court moved next to the instructions requiring the search be performed by a third party, separate from the investigation and behind a firewall. Responding to the State's contention that the instructions essentially remove any application of the plain view doctrine, the majority differentiates between viewing evidence and seizing it. The plain view doctrine, it explains, touches upon seizures, not searches, by focusing on what action is permissible after incriminating evidence has been viewed, not before. Since the instruction requiring the search to be performed by third party screeners would not allow officers to view such evidence, the plain view doctrine has no application. Justice Burgess (with whom Chief Justice Reiber joins in the dissent) equates the practice of having police officers not tied to the investigation conduct the search as being anything other than an invasion of privacy by the government to the "old adage of being 'just a little bit pregnant.'" Regardless of which officer performs it, a search is a search is a search, and evidence in plain view is in plain view whether it is seized or not.

Though the minority opinion doesn't seem to dismiss entirely the possibility that technology can pose a challenge to traditional Fourth Amendment search and seizure analysis, it fails to see this case as posing such a problem. The minority doesn't distinguish between the physical world and the metaphysical one but rather views a computer as merely just another device for information. "What the State seeks to look for, and where, seems hardly different from a search for files in a cabinet, papers in a desk, drafts in a checking account or letters in a box." What matters are the protections afforded by the Fourth Amendment. Once those are afforded, the intrusion of one's privacy is deemed

reasonable and the plain view doctrine is in play. The minority also points out that the majority is trying to have it both ways by upholding conditions effectively negating application of the plain view doctrine while simultaneously ruling that the judicial officer issuing the warrant exceeded his authority in refusing to apply. "Eliminating plain view ad hoc in a particular search through the *ex ante* artifice of a separate and gagged search team achieves exactly what the majority acknowledges is improper, leaving the magistrate 'to disregard the considered limitations of the law' (like the court's lack of authority to proscribe plain view), and conferring 'on a judicial officer the authority to pick and choose what legal doctrines would apply to a particular search' (as in commanding police to ignore evidence in plain view in a computer search, while allowing plain view discovery in a house or office search)."

But the majority holds that not all searches are created equal as there are real world consequences to who sees personal information. It is precisely the unique capacity and storage capabilities of computers and the potential exposure of vast personal information that their search pose that necessitates a different set of rules. The "massive storage capacity of modern computers creates a high risk of overbroad, wide-ranging searches and seizures." Criminals after all are not likely to have a folder entitled "identity theft" lying around on their desktop. A computer keeps a record of every search and every file created. Searching that history subjects to view all unrelated information, meaning that everything is in virtual plain view and therefore subject to seizure.

Returning finally to the condition requiring the search to be performed by an outside third party, the State argues that the suspect's privacy rights are materially well advanced to justify their imposition. The minority agrees, taking the position that an invasion to one's privacy occurs when anyone sees any personal information without his or her permission, so it doesn't matter if an officer tied to the investigation sees it. The majority takes a more nuanced approach to this analysis by focusing instead on the relational aspects of one's privacy interests. By means of demonstration, let's say you really like those pictures on the internet of cats with the funny sayings ... a lot. Now if some stranger in Tulsa, Oklahoma logs onto your work computer and sees a thousand of those pictures in your saved files, that probably won't affect you because you don't have a relationship with that person. Replace that person with your employer and you'll probably have a difficult time explaining what you do all day at work. The point the majority makes is that of course it matters who sees what. People have relationships, and the nature of what is discovered has an impact on them, particularly when that relationship is with a police officer. "A citizen's relationship with a police officer engaged in an investigation is asymmetric in power and laden with potential consequences. Unlike virtually any other person, an investigating police officer has the power to place a citizen at the mercy of the State." Having that search filtered through someone, whether it be a computer expert, court or special master, limits the potential negative consequences of the invasion suffered. "There is interplay between probable cause, particularity, and reasonableness that judicial officers reviewing a warrant application must consider in authorizing a form of privacy invasion."

One wonders if the majority of the Court will apply this same practical approach to privacy interests in other realms. In the meantime, enjoy those funny cat pictures without fear of discovery, at least not by investigating officers. The decision is archived at http://info.libraries.vermont.gov/supct/current/op2010-479.html.

Garrett Baxter, Staff Attorney II
VLCT Municipal Assistance Center