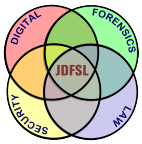

THE JOURNAL OF
DIGITAL FORENSICS,
SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 7 | Number 4 Article 2

2012

"Preemptive Suppression" – Judges Claim the Right to Find Digital Evidence Inadmissible Before It Is Even Discovered

Bob Simpson
Champlain College

“Preemptive Suppression” – Judges Claim the Right to Find Digital Evidence Inadmissible Before It Is Even Discovered

Cover Page Footnote

1. Robert V. Simpson, Jr., graduated from Colgate University (BA, 1967), Vermont Law School (JD, 1978) and served as a prosecutor in Chittenden County (Vermont) between 1979 and 81 and again between 1994 and 2006. 2. In Re Appeal of Application for Search Warrant, No. 2010-479 (S. Ct. Vt. Filed December 29, 2010) 3. The prosecutors' first argument is that Vermont judges lack legal authority to impose these preconditions. This dispute over whether judges have the legal authority to impose these restrictive preconditions has become, in part, a battle by proxy between law professors. Prosecutors rely on the analysis of George Washington University Law Professor, Orin Kerr, who argues that judges do not have legal authority to impose conditions on how officers will execute search warrants. Orin S. Kerr, Ex Ante Regulation of Computer Search and Seizure, 96 Va. L. Rev. 1241 (2010) Two national organizations, the Criminal Law Reform Project of the ACLU Foundation and the Electronic Frontier Foundation (EFF) responded to the prosecutors' reliance on Professor Kerr by countering with the March 2011 reply to Professor Kerr by Professor Paul Ohm. Brief of ACLU and EFF, filed in Docket No. 2010-479 on June 17, 2011 at 15. Professor Ohm contends these conditions are not only lawful, but necessary. Paul Ohm, Massive Hard Drives, General Warrants, and the Power of Magistrate Judges, 97 Va. L. Rev. 1, 4 (March, 2011) 4. The Vermont conditions are: 1. As a condition for receiving a search warrant to search the subject computer, the State cannot rely upon the "plain view doctrine" to seize any electronic records other than those authorized by this warrant. That is, any digital evidence relating to criminal matters other than the identity theft offenses, may not be seized, copied, or used in any criminal investigation or prosecution of any person. 2. Inspection and investigation of the subject computer must be done by either an independent third party or specially trained computer personnel who are not involved in the investigation while staying behind a firewall, that is, in the absence of other agents of the State, and subject to a ban on copying or communicating to any person or the State any information found on the subject computer other than digital evidence relating to identity theft offenses. 3. Any digital evidence relating to the offenses must be segregated and redacted before it is provided to the State, no matter how intermingled it is. 4. If the segregation is performed by State computer personnel, it is a condition of this warrant that the computer personnel will not disclose to the State investigators or prosecutors any information other than that which is the target of the warrant, that is, digital evidence of the identity theft offenses. 5. The search protocol employed must be designed to uncover only the information for which the State has probable cause, that is the aforesaid alleged offenses, and only that digital evidence may be provided to the State. Techniques to focus the search should include but are not limited to, specific time periods relevant to the alleged criminal activity, key word searches, and limiting the search to specific file types. 6. The government has at its disposal sophisticated hashing tools that allow identification of well-known illegal files (such as child pornography) that are not at issue in this case. These and similar search tools may not be used without specific authorization by the court. 7. Information relevant to the targeted alleged activities may be copied to other media to provide to State agents. No other digital evidence may be so copied. 8. The government must return non-responsive data, keeping the court informed about when it has done so and what it has kept. 9. Any remaining copies of the electronic data must be destroyed absent specific judicial authorization to do otherwise. 10. Within the time specified in the warrant, the State must provide the issuing officer with a return disclosing precisely what data it has obtained as a consequence of the search, and what data it has returned to the party from whom it was seized. The return must include a sworn certificate that the government has destroyed or returned all copies of data that it is not entitled to keep. In re: Application for Search Warrant Eric Gulfield Computer, Chittenden Superior Court , Amended Order at 1 (Dec. 22, 2010)

Printed Case (PC) 3-4 5. Judge Michael Kupersmith is a respected trial judge with well-over twenty years of experience in Vermont's Criminal Division. 6. In re: Application for Search Warrant Eric Gulfield Computer, Chittenden Superior Court, Amended Order at 1 (Dec. 22, 2010) Printed Case (PC) 3-4 "The application to search the computer belonging to Eric Gulfield is granted subject to the conditions listed herein. In setting these conditions, the Court has been guided by United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 9th Cir. (2009)." 7. The 9th Circuit is the largest Federal Circuit Court of Appeals in the United States. It covers federal courts in Arizona, California, Nevada, Montana, Oregon, Idaho, Washington, Alaska and Hawaii as well as Guam and the Northern Marianna Islands. 8. United States v. Comprehensive Drug Testing, Inc.,579 F.3d 989 (9th Cir.2009) 9. CDT II, 579 F.3d 989, 1000 10. Id 11. Chief Judge Kozinski summarized the "guidance" that magistrates "must be vigilant" in observing: 1. Magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases. 2. Segregation and redaction must be either done by specialized personnel or an independent third party. If the segregation is to be done by government computer personnel, it must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant. 3. Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora. 4. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents. 5. The government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept. United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1006 (9th Cir.2009) (internal citations omitted) 12 US v. Comprehensive Drug Testing Inc., 621 F3d 1162,1176 (9th Cir 2010) (CDT III) 13. CDT III at 1180 14. CDT III at 1178 15. In the Matter of the United States Of America's Application For A Search Warrant To Seize And Search Electronic Devices From Edward Cunnius, 770 F. Supp. 2d 1138, 1139 (W.D. Washington, 2011) 16. According to Detective Lt. Kris Carlson of the Burlington (Vermont) Police Department, an officer with long experience as a computer forensic investigator, Vermont police officers have specific objections to nearly all of the CDT conditions. But their overriding general objection is that, although they well understand that computers can contain huge amounts of private information, they see no reasonable justification for the imposition of vastly greater restrictions on searches of computers than restrictions on searches of homes, which are generally considered the most private of private places. Recorded interview with Detective Lt. Kris Carlson, Director of Vermont's Internet Crimes Against Children (ICAC) Task Force in Burlington, Vermont on July 19, 2011 17. Paul Ohm, Massive Hard Drives, General Warrants, and the Power of Magistrate Judges, 97 Va. L. Rev. 1, 3, 8 (March, 2011) 18. 97 Va. L. Rev. 8 19. Bryan Weir, It's (Not So) Plain to See: The Circuit Split on the Plain View Doctrine in Digital Searches, 21 Geo. Mason U. Civ. Rts. L. J. 83, 113 (Fall 2010); James Saylor, Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches, 79 Fordham Law Review 2809 (May, 2011); James Stinsman, Computers and Searches, Rethinking the Applicability of the Plain View Doctrine, 83 Temple Law Review 1097, 1120 (Summer 2011) and Matthew Dodovich, The Plain View Doctrine Strikes Out In Digital File Searches, 6 ISLP 659, 691 (Summer, 2011) 20. E.g., summaries of statements from customers and neighbors 21. The U.S. Supreme Court has said that "probable cause" means that there is a "fair probability" that contraband or evidence of a crime is at a particular place. Illinois v. Gates, 462 US 213, 238 (1983) 22. The officer must also prepare an application but that document merely gives the judge an outline of the substantive information developed in the warrant and the supporting affidavit. 23. The judge, in turn, "must" grant the warrant if there is probable cause to believe that the evidence of the crime identified in the warrant is located at the place identified in the warrant. The applicable Court Rules are Fed. R. Crim. P 41 (d) (1) which says: (1) In General. After receiving an affidavit or other information, a magistrate judge – or if authorized by Rule 41(b), a judge of a state court of record – must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device; and Vt. R. Crim P 41 (c) which says (1)

Probable Cause. A judicial officer shall issue the warrant if the judicial officer is satisfied that there is probable cause to believe that grounds for the application exist based upon an affidavit or affidavits or sworn testimony or both." 24. The warrant which is now before the Vermont Supreme Court says: "To: Det. Michael Warren and any Vermont Law Enforcement Officer You are hereby commanded to search:" (emphasis in the original) 25. "The application to search the computer belonging to E.G., is granted subject to the conditions listed herein. In setting these conditions, the Court has been guided by United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 9th Cir. 2009)." Amended Order, In re: Application for Search Warrant E_G_ Computer, December 22, 2010 at 3 26. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." 27. Horton v. California, 496 US 128 (1990) 28. Crimes Act 1914 Section 3F - http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/s3f.html 29. "The problem can be stated very simply: There is no way to be sure exactly what an electronic file contains without somehow examining its contents either by opening it or looking, using specialized forensic software, keyword searching or some other such technique. But electronic files are generally found on media that also contain thousands or millions of other files among which the soughtafter data may be stored or concealed. By necessity, government efforts to locate particular files will require examining a great many other files to exclude the possibility that the sought-after data are concealed there." CDT II, 579 F3d at 1004. 30. See, Orin S. Kerr, Searches and Seizures in a Digital World, 119 Harv. L .Rev. 531, 568-71 (2005) 31."Thus, the scope of a lawful search is 'defined by the object of the search and the places in which there is probable cause to believe it may be found." Maryland v. Garrison, 480 US 79, 84(1987) (quoting US v. Ross, 456 US 798, 824 (1982) The scope of the search in the hypothetical is limited by the "object" of the search – evidence of the crime of sale of marijuana, the crime identified in the warrant and a crime for which the officer had probable cause. The officer exceeded the scope of the warrant because he was looking for evidence of the crime of sexual exploitation of a child – a crime that was not identified in the warrant, and a crime for which he did not have probable cause. 32. "It is, of course, an essential predicate to any valid warrantless seizure of incriminating evidence that the officer did not violate the Fourth Amendment in arriving at the place from which the evidence could be plainly viewed." Horton, 496 US at 136. 33. 579 F3d at 997-999, 1005 34. 579 F3d 998 35. Id 36. 579 F3d 1006 37. U.S. v. Farlow, 2009 WL 4728690 (D. Me. 2009, slip opinion p. 6 fn3) 38. In Re Appeal of Application for Search Warrant, No. 2010-479 (S. Ct. Vt. Filed December 29, 2010), affidavit of Detective Michael Warren in support of application for search warrant, Printed Case (PC) 8-9 39. The investigator, Detective Warren, does have training and experience in computer forensic investigations. Id. 7 40. Vermont officer/examiners are taught to confine the scope of their searches to the evidence delineated in the search warrant. If they do open a file that reveals evidence of another crime "in plain view," they apply for another warrant. Interview with Detective Lt. Kris Carlson, Director of Vermont's Internet Crimes Against Children (ICAC) Task Force in Burlington, Vermont on July 19, 2011 41. 97 Va. L. Rev. 5 42. Id 43. Paul Ohm, Massive Hard Drives, General Warrants, and the Power of Magistrate Judges, 97 Va. L. Rev. 11 (March, 2011) 44. 97 Va. L. Rev. 4 45. Whether the place to searched, is a car, a home or a computer, the officers always "seize" the place to be searched first in the sense that they take control of that place before they begin searching through non-incriminating objects and information for evidence of the crime identified in the warrant. The big difference in computer searches is that the search of the copied hard drive usually takes places offsite. 46. 97 Va. L. Rev. 7 47. 97 Va. L. Rev. 8 48. US v. Upham, 168 F3d 532, 535 (1st Cir., 1999) 49. Fed. R. Evid. 401; Vt. R. Evid. 401 50. Fed. R. Evid. 402; Vt. R. Evid. 402 51. Weeks v. US, 232 US 383 (1918) 52. Mapp v. Ohio, 367 US 343 (1961) 53. US v. Herring, 555 US 135, 141 (2009) 54. Hudson v. Michigan, 547 US 586, 591 (2006) 55. Id. 56. "Our cases show but-for causality is only a necessary, not sufficient, condition for suppression." 547 US at 592 57. According to one source, there are roughly 175,000 "suppression hearings" held in our courts in the U.S. each year on Fourth Amendment issues alone. Joel Samaha, Criminal Procedure, 7 th edition 361 (2008) 58. U.S. v. Kim, 677 F.

Supp. 2d 930, 950(S.D. Texas, 2009) 59. 579 F3d at 1006 60. 2. Inspection and investigation of the subject computer must be done by either an independent third party or specially trained computer personnel who are not involved in the investigation while staying behind a firewall, that is, in the absence of other agents of the State, and subject to a ban on copying or communicating to any person or the State any information found on the subject computer other than digital evidence relating to identity theft offenses. 3. Any digital evidence relating to the offenses must be segregated and redacted before it is provided to the State, no matter how intermingled it is. 4. If the segregation is performed by State computer personnel, it is a condition of this warrant that the computer personnel will not disclose to the State investigators or prosecutors any information other than that which is the target of the warrant, that is, digital evidence of the identity theft offenses. 61. The federal law says: "A search warrant may in all cases be served by any of the officers mentioned in its direction or by an officer authorized by law to serve such warrant, but by no other person, except in aid of the officer on his requiring it, he being present and acting in its execution." 18 USC 3105 Vermont Rule of Criminal Procedure 41 (c) (5) likewise says the warrant must be executed by a law enforcement officer: ". . . The warrant shall be directed to a law enforcement officer of the state of Vermont authorized to enforce or assist in enforcing any law thereof. The warrant shall command the officer to search the person or place named for the property or other object specified and seize the property or object and, if appropriate, the person specified." 62. Vermont Rule of Evidence 502; Federal Rule of Evidence 502 63. E.g., Comcast, Yahoo! 64. E.g., businesses that store and process electronic billing information for physicians 65. 18 USC 2703 (g) 66. U.S. Attorneys Criminal Resource Manual, part 59-Guidelines on Methods of Obtaining Documentary Materials Held by Third Parties, 28 C.F.R. Part 59, § 59.1 67. Investigators may proceed by search warrant – but only when using a subpoena would "substantially jeopardize the investigation. Id. 68. I worked for roughly fifteen years as a prosecutor in Vermont. I am aware of only two cases when it was necessary to use an independent third party to execute the search warrant in order to sort out material that was protected by attorneyclient privilege. One of the two cases involved a computer warrant. (U.S. v. Hunter, fn. 70 – below) 69. U.S. v. Taylor, 764 F. Supp. 2d 230, 232-36 (D. Me. 2011) 70. U.S. v. Hunter, 13 F. Supp. 2d 574 (D. Vt. 1998) involved a computer search warrant of records of an attorney who published a legal newsletter. The search raised both attorney-client privilege issues and Privacy Protection Act questions. The US Attorney for Vermont designated a team consisting of an attorney and officers who were not involved in the criminal investigation ("taint team") to conduct the search and sort out evidence that the investigating officers were authorized to view under the warrant. 71. CDT II, 579 F3d 989, 1013 (Callahan, Circuit Judge, concurring in part, dissenting in part) 72. Despite the apparent requirements of Rule 41 of the Vermont Rules of Criminal Procedure, Condition 2 does not require the "independent expert" to be a law enforcement officer. 73. The case is US v .Abbell, 914 F. Supp. 519 (S.D. Fla. 1995). The delay is reported in Black v. US, 172 FRD 511, 514 n.4 (S.D. Fla. 1997) 74. 172 FRD 516 75. New York State Police conducted the initial investigation and then gave information that they had to Burlington, Vermont Police because it appeared the person suspected of the crime lived in Burlington. In Re Appeal of Application for Search Warrant, No. 2010-479 (S. Ct. Vt. Filed December 29, 2010) PC 5- 11 76. Id 77.PC 6-7 78. Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches, 79 Fordham L. Rev. at 2856 79. 79 Fordham L. Rev. at 2857 80. Id.

"PREEMPTIVE SUPPRESSION" – JUDGES CLAIM THE RIGHT TO FIND DIGITAL EVIDENCE INADMISSIBLE BEFORE IT IS EVEN DISCOVERED

Bob Simpson, JD[1]
Champlain College

Vermont state prosecutors have asked[2] the Vermont Supreme Court to end a state trial judge's practice[3] of attaching conditions[4] to computer warrants. The Vermont judge's[5] conditions are drawn from five conditions[6] established in the 2009 decision of the 9th Circuit Court of Appeals[7] in the Comprehensive Drug Testing, Inc. case (*CDT* II).[8] This is the first time the validity of the "*CDT* conditions" will be decided by a state court of final jurisdiction in the United States.

The *CDT II* majority reacted to what it termed "an obvious case of deliberate overreaching by the government in an effort to seize data as to which it lacked probable cause."[9] Determined "to guard against such unlawful conduct in the future[10]",Chief Judge Alex Kozinski, author of the majority opinion, set out five conditions, or "guidance,[11]" that magistrate judges were to require law enforcement officers to agree to, before the judge signed a computer warrant. The 9th Circuit withdrew these conditions from the majority opinion in September 2010 (*CDT* III). But, it reaffirmed its conclusion that government agents had violated the Fourth Amendment to the United States Constitution in the *CDT* case. And, it repeated its concern that the "pressing need of law enforcement for broad authorization to examine electronic records … creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant."[12]

The *CDT* conditions did not disappear when they were withdrawn from the majority opinion in *CDT III*. Chief Judge Kozinski made them part of his concurring opinion, apparently to emphasize their continuing importance.[13] Four other judges joined in his concurring opinion.[14] Five months after that, a federal magistrate in the Western District of Washington reaffirmed the continuing vitality of the *CDT* conditions when he refused to sign a computer warrant after federal prosecutors refused to agree to the two most controversial of these pre-conditions. Prosecutors seeking a warrant to search computers for evidence of trafficking in counterfeit goods and criminal copyright infringement *refused* to: (1) "forswear reliance on the plain view doctrine" (*CDT* Condition1) and (2) conduct the search with "a filter team to separate from the investigative agents information that is outside the scope of the warrant" (*CDT* Condition 2).

The judge responded by refusing to grant the search warrant.[15]

This article focuses on these two conditions (*CDT* Conditions 1 and 2). I contend they are gratuitously damaging to fair and effective law enforcement in Vermont[16] and anywhere else they are adopted.

- *CDT* Condition 1: This condition requires all "case agents" (case investigators) seeking a warrant to search computers to "waive reliance upon the plain view doctrine" before a judge will sign the warrant. This amounts to what I call "preemptive suppression."
  The *CDT* majority evidently concluded that granting case investigators judicial authority to search computers will *always* create an intolerable risk these officers will abuse this authority. The majority presumed that investigators would use the warrant as "cover" to convert the right to search for evidence of the *specific crime* identified in the warrant into an illegal "general warrant" enabling them to look through every file on the computer for *everything* that may be damaging to the computer user. The majority decided to act preemptively to eliminate this risk before the search even takes place. It did so by ordering magistrate judges in the 9th Circuit to require case investigators and prosecutors to agree, as a condition to obtaining a computer warrant, that the government *will never use any "plain view" evidence* obtained during the course of the computer search in any criminal case – regardless of whether evidence is obtained lawfully. As a result, evidence of other potentially serious crimes (e.g., murder, kidnapping, extortion) is "suppressed" – excluded from use in any prosecution– before it is even gathered.
- *CDT* Condition 2: Case investigators applying for a computer warrant must also agree, as a condition to obtaining the warrant, they will play no further role in the search of the computer(s) identified in the warrant. The "segregation" of digital evidence that tends to prove, or disprove, the crimes identified in the warrant from evidence that is not "the target of the warrant" is to be done, either by "an independent third party" expert or law enforcement computer experts. In other words, the case investigators, the people who know the most about the specific criminal activity that is the subject warrant, can play no part in the search and no role in deciding what digital evidence is relevant to their investigation. This will mean delay, added expense and increase the likelihood that the search will be broader than necessary. It will also increase the likelihood that important evidence will be overlooked.

Professor Paul Ohm of the University Colorado Law School sees the *CDT* conditions as part of a "trend emerging" among federal magistrate judges who are attempting to "creatively superintend" how computer warrants are drafted and executed.[17] Professor Ohm sees the *CDT* conditions as an example of the

"subtler, more nuanced approaches" judges must adopt in order to solve the "special problems" created by computer searches.[18] Professor Ohm is not alone. He is joined by at least four other law review commentators who support CDT conditions 1 and 2.[19]

I have a different view. There is no dispute that computer searches pose a special challenge for police, prosecutors and judges who must insure that searches for digital evidence do not overwhelm individual rights protected by the Fourth Amendment to the United States Constitution. However, *CDT* conditions 1 and 2 not only require preemptive suppression; but, they also bar case investigators from taking any part in deciding whether particular pieces of digital evidence are relevant to crimes they are investigating. These conditions are (1) not "subtle;" (2) not "nuanced" and (3) not supported by either the evidence, or the law.

I begin (below) with a brief summary of the process of obtaining a search warrant, followed by an explanation of the "special problem" that Conditions 1 and 2 are intended to address. The article goes on to explain why Condition 1, which bars the prosecution from using an entire class of evidence before the computer warrant is even signed, is an unnecessary, radical remedy that is not founded on the evidence or the law. The second part of this two-part article deals with Condition 2. It explains that by barring investigators from taking part in the search, Condition 2, again without any legal basis, has the unwarranted effect of treating all digital evidence obtained through a computer warrant as though it is protected by attorney-client privilege. This creates more problems than it solves because it means unnecessary expense, delay and loss of relevant evidence.

THE PROCESS OF OBTAINING A SEARCH WARRANT

On a basic level, the process for obtaining a warrant to search a computer is the same as the process for obtaining a warrant to search a home or any other place where a person has a "reasonable expectation of privacy." The officer assigned to investigate the crime (e.g., sale of cocaine) must write an affidavit that sets out facts and circumstances[20] developed during the officer's investigation that demonstrate there is probable cause[21] to believe that evidence of the crime under investigation is located on the suspect's computer, which is, in turn, located at a specific place. The investigating officer must also write a proposed search warrant that identifies "with particularity" the place to be searched and the evidence to be seized. The "on call" prosecutor then reviews these documents[22]. Once the prosecutor is satisfied that the documents meet legal requirements (e.g., Fourth Amendment and state and federal rules governing search warrants), the prosecutor contacts the "on call" judge.

The judge then conducts an independent review of the officer's documents. If

the judge is satisfied that the documents are legally sufficient, the judge will sign[23] the warrant authorizing the investigating officer[24] to conduct a search of the place described in the warrant for the evidence described in the warrant. In the computer warrant case now before the Vermont Supreme Court, the Vermont judge attached the *CDT* conditions to the warrant after he signed it.[25] Prosecutors then appealed to the Vermont Supreme Court.

THE "PLAIN VIEW DOCTRINE"

The Fourth Amendment[26] to the US Constitution prohibits "government agents" (e.g., police officers, federal law enforcement agents) from searching for and/or seizing evidence that is located in a place where an individual has a "reasonable expectation of privacy" unless the government agent has a warrant to conduct the search – a warrant authorized by a neutral judge.

There are, however, several well-recognized judicially-created exceptions to this "warrant requirement." The so-called "plain view doctrine" is one of these exceptions[27]. It says that a law enforcement officer does not need a warrant to seize evidence if: (1) the officer is legally in a position to observe something - because he has a search warrant to search a computer, for instance; (2) that officer has the lawful right to access the object in "plain view" – when he opens a file during the computer search, for instance, and (3) the incriminating nature of the evidence is "immediately apparent" – the file she opens is an image of a child being sexually assaulted, for instance. Under the plain view doctrine, the officer is entitled to seize (copy) the image without a warrant because the original warrant put him in a position to observe the file legally and the incriminating nature of the opened file is immediately apparent.

The plain view doctrine is not radical. Other countries have adopted rules similar to this US rule allowing a law enforcement officer who is lawfully in a position to observe, and seize, evidence whose "incriminating nature is immediately apparent." In Australia, for example, Crimes Act 1914, Section 3F (1) (d) (ii) authorizes an officer executing a search warrant for evidence of a particular crime to seize evidence that is not listed in the warrant if s/he "believes on reasonable grounds" it is "evidential material in relation to another offense that is an indictable offence."[28]

WARRANTS TO SEARCH COMPUTERS CAN BECOME "GENERAL WARRANTS" ENABLING THE GOVERNMENT TO SEARCH COMPUTERS FOR ANYTHING ITS AGENTS CARE TO LOOK FOR

Computer searches create the *potential* for officers to take advantage of the fact that a computer user can hide evidence of a crime anywhere on a computer [29] and turn legal warrants into illegal "general warrants[30]." That is, they can exploit warrants that give them legal authorization to search computers for evidence that a *specific* person has committed a *specific* crime and use these warrants as a means to rummage through a person's computer in search of evidence of *any* crime.

Assume an officer has probable cause to believe there is evidence of possession of marijuana on X's computer and that he obtains a valid warrant to search a computer for evidence of sale of marijuana. Assume also that the officer *suspects* that the computer's owner has committed another crime – a more serious crime such as sexual exploitation of a child – *but lacks the "probable cause*" that would give him a legal basis under the Fourth Amendment to obtain a second warrant to lawfully search for the sexual exploitation evidence. This officer, can, nonetheless, lawfully go through every file on the computer looking for evidence of sale of marijuana, while hoping, at the same time, that he will uncover evidence of this crime, or, for that matter, any other crime.

Next, assume the officer does open a file that contains an image that makes it immediately apparent that the computer user has engaged in the sexual exploitation of a child. The officer can use the "plain view" exception to the Fourth Amendment search warrant requirement to justify "seizing" this evidence of this more serious crime. The officer can then use the evidence of child exploitation that he found in "plain view" to establish the "probable cause" necessary to obtain a second search warrant to lawfully look for more evidence that the computer user has engaged in sexual exploitation of a child.

On its face, this is all legal; but, a violation of the computer owner/user's Fourth Amendment rights may have already occurred.

The original "marijuana warrant" gave the officer the legal right to open all files to search for evidence of the sale of marijuana. But, suppose the officer never had any interest in the marijuana case and he never had any intent to search X's computer for marijuana evidence, or that he lost interest in the marijuana case shortly after the warrant was granted. Instead, he used the "probable cause" he *did have,* solely as a means to get a warrant that gave him access to X's computer. Suppose he then opened every file to search for evidence of child sexual exploitation, or other crimes for which he *did not have* probable cause.

Under those circumstances, the officer violated X's Fourth Amendment right to be free from unreasonable searches from the time he began executing (conducting) the search because he deliberately exceeded the scope of the

warrant (which limited him to searching for "marijuana evidence"[31]) as soon as he began the search. He did not have the right to rely on the plain view doctrine. Opening the file put him a position to see the exploitation evidence in "plain view." But, he did not get into the position to view the "exploitation evidence" legally[32]. He opened the file in which X had a reasonable expectation of privacy unlawfully. He opened it knowing he was looking for evidence of a crime for which he did not have probable cause – a crime that was not identified in the warrant he did have. It was an illegal warrantless search, which, in turn, made the "plain view" seizure of the evidence exploitation illegal.

The officer executing the computer warrant made a conscious decision to violate the Fourth Amendment by exploiting: (1) the authority of the warrant; (2) the unique nature of digital evidence and (3) the plain view doctrine to search for, and seize, evidence he which he knew he did not have probable cause.

THERE IS NO EVIDENCE OF WIDESPREAD POLICE MISCONDUCT THAT WOULD SUPPORT IMPOSITION OF CONDITIONS 1 AND 2

The unique nature of digital evidence (including the capacity to store enormous amounts of information) does create the potential for officers who are *executing* computer warrants to violate the Fourth Amendment and convert them into "general warrants" that can result in massive violations of privacy. But, this *potential* for privacy violations will not harden into the *reality* of a privacy violation unless an officer *deliberately* violates the law. So far, no court, or commentator, has come forward with evidence that justifies the presumption, implicit in Conditions 1 and 2, that *all* investigating officers who execute computer warrants will deliberately violate the Fourth Amendment by searching for evidence of crimes for which they do not have probable cause and then purporting to lawfully seize this evidence under the plain view doctrine.

Chief Judge Kozinski wrote the *CDT* conditions in response to *one incident* of "unlawful conduct" involving federal agents investigating the use of steroids in Major League Baseball. According to Judge Kozinski's majority opinion in *CDT II*, at least one of the agents who executed computer search warrants at drug testing facilities in California and Nevada violated the privacy rights of hundreds of individuals[33] by deliberately searching for evidence of crimes for which he did not have probable cause; and then when he found this evidence, exploited the "plain view doctrine" to seize it illegally.

Judge Kozinski explained that he had no quarrel with the proposition that because computer users can hide evidence of a crime anywhere on a computer, officers may have to carefully examine every file to insure they find all evidence they were authorized to search for.[34] But, he predicted that this meant that "anything the government chooses to seize" will eventually "come into plain

view." And this, in turn, he said, created a "powerful incentive" for officers to "seize more rather than less" and then take "everything back to the lab" to see what investigators "may stumble upon."[35]

To eliminate this "powerful incentive" to bring everything into "plain view" in order to see what investigators" may stumble upon," Judge Kozinski told magistrate judges in the Ninth Circuit to insist that case investigators "waive reliance upon the plain view doctrine in digital evidence cases" (Condition 1) *before* these judges approved a warrant to search a computer[36].

The effect of Condition 1 was stunning. It insured that no digital evidence obtained through the plain view doctrine in a computer search could ever be used in any criminal prosecution, regardless of whether it was obtained legally-in fact, without any specific consideration of whether it was obtained legally.

Why? The Court was clearly frustrated by what it saw as the cynical exploitation of the doctrine by case investigators in the CDT case. But why order preemptive suppression of all digital evidence that may ever be seized under the plain view doctrine in any computer search warrant case in the Ninth Circuit based on a single instance of "deliberate overreaching" by officers? What is the evidence of widespread abuse of the plain view doctrine in computer searches that justifies establishing what is, in effect, a judicial presumption that officers who execute computer search warrants will deliberately violate the Fourth Amendment by exploiting the plain view doctrine?

The Ninth Circuit did not cite any. No one else has either.

Judge John Woodcock, Chief U.S. District Judge in Maine, pointed out there was no evidentiary basis for such a presumption when he rejected, as "unwise," the CDT II conditions just four months after the decision was issued:

> The *CDT* protocols impose extraordinary precautions against police misconduct for all applications for a warrant to search a computer, assuming misconduct will be the rule, not the exception. There is no evidence that police disobedience of search warrant limitations is so widespread to compel such onerous pre-issuance procedures, and at the very least the more traditional remedies should be tried first.
>
> The judicial directive to forswear in advance the plain view doctrine, placed in a different context, is equivalent to demanding that a DEA investigative team engaged in the search of a residence for drugs promise to ignore screams from a closet or a victim tied to a chair.[37]

To see just how unwise Condition 1 is, please consider this hypothetical based on the warrant now being considered by the Vermont Supreme Court. The warrant authorizes officers to search for evidence of one crime – "identity theft."

It authorizes "Det. Michael Warren," the detective who conducted the investigation and wrote the affidavit in support of the warrant, to search the premises and seize "records" in "whatever form they are found" including records stored on computers.[38]

Assume Detective Warren searches *paper records* pursuant to the warrant – e.g., a three-ring notebook or a stack of papers – for evidence of the crime of identity theft. Assume further that it becomes "immediately apparent" as he turns a page that he is looking at a list of illegal drug sales. He would be authorized under the plain view doctrine to seize that record and use it as the basis for an affidavit to secure another warrant to search the premises for evidence of the additional crime of delivery of illegal drugs. But, assume instead, that he opens a *Word file* on a copy of a hard drive[39], seized pursuant to the same warrant and it is "immediately apparent" that he is looking at a list of the same illegal drug sales. He will have to *ignore* this *digital* evidence. This is because, under Condition 1, he cannot "seize copy or use" the cocaine transactions evidence "in any criminal investigation or prosecution of any person" because it was seized from a computer under the plain view doctrine.

Detective Warren has not violated the Fourth Amendment in conducting either the paper search, or the computer search. In the search of the paper "records," evidence obtained under the plain view doctrine may be used to obtain a search warrant to conduct an independent investigation into cocaine sales. The paper record will also be admissible for consideration by a jury if charges of cocaine sale are brought. However, the same evidence in digital form obtained during the search of computer "records" cannot be used by the prosecution for any reason. Under Condition 1, it has been suppressed before it is even found.

There is no evidence of widespread abuse by case investigators executing computer warrants in Vermont[40]. Despite this, the Vermont Judge has adopted *CDT* Condition 1 – a condition founded on the "evidence-free" presumption that investigators will deliberately violate the Fourth Amendment when they execute computer warrants.

THE LAW DOES NOT SUPPORT THE IMPOSITION OF THE *CDT* CONDITIONS

Professor Ohm makes a different, yet equally startling claim. He focuses, not on officer misconduct in executing computer warrants, but on the invalidity of the warrants themselves. Professor Ohm says that "almost every" computer warrant violates the Fourth Amendment.[41] Under his analysis, judges not only have the legal authority to impose *CDT II* type conditions, they have the obligation to do so in order to "compensate for the lack of probable cause and particularity – not merely to ensure reasonable execution – in almost every computer case."[42]

Professor Ohm's tone is apocalyptic. He says "computer search warrants are the closest things to general warrants we have confronted in the history of the Republic"[43] and that *CDT* conditions "are designed to cure the *manifest lack of probable cause and particularity in almost every* computer case." (Professor Ohm's emphasis)[44]

Surely it is an overstatement to say that "almost every" one of the thousands of computer warrants issued by state and federal judges in the U.S. every year are not supported by affidavits establishing a "fair probability" that evidence of the crime(s) identified "with particularity" in the warrant will be found on the computer devices at a place, identified with "particularity," in the warrant.

As it turns out, Professor Ohm is not arguing that judges are routinely granting computer warrants that lack particularity and probable cause. Instead, he seems to be saying that we have reached a point at which the sheer volume of private, non-relevant information "commingled" with evidence of the crime identified in the warrant is so overwhelming that, as a matter of law, the sheer volume of this "innocent" information somehow dilutes "particularity" and extinguishes the legal vitality of the finding of probable cause that justified the warrant in the first place.

Officers executing a search warrant will always observe[45] "non-incriminating" objects, or information, as they search for evidence of crimes identified in the warrant whether it is a search of a car for evidence of illegal drugs, a house for evidence of stolen jewelry or paper business records for evidence of fraud. Officers will always have to "segregate" information that tends to prove, or disprove, the crime(s) identified in the warrant from large amounts "commingled" information that is not related to the crimes identified in the warrant.

Professor Ohm is right, though, when he says that officers searching a computer will have the opportunity to view vast amounts of "sensitive" commingled evidence that will exceed, by many orders of magnitude, the quantity of commingled evidence they would be likely to view in executing any other type of warrant.[46] He is also right that the "commingling" of vast amounts of "non-incriminatory" information with information that is evidence of a crime is an

important part of the "special problem" of computer searches.

But, to date, judges have not concluded, as Professor Ohm evidently has, that the fact that computer warrants create an opportunity for case investigators to view a vast amount of private, non-relevant data as they search for evidence of the crime identified in the warrant, somehow translates into a "manifest" lack of probable cause or an "intractable failure of particularity."[47]

As the First Circuit put it, a search of computer is not "inherently more intrusive" than a search of a home. And, according to the court, an affidavit establishing probable cause to believe there is evidence of the crime identified somewhere on a computer device establishes a constitutionally "sufficient chance of finding some needles in the computer haystack" to meet the "particularity" requirement:

> As a practical matter, the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the images. A sufficient chance of finding some needles in the computer haystack was established by the probable-cause showing in the warrant application; and a search of a computer and collocated disks is not inherently more intrusive than the physical search of an entire house for a weapon or drugs.[48]

Moreover, the Fourth Amendment, as interpreted by the US Supreme Court, simply cannot be read to support Professor Ohm's claims that the sheer volume of commingled information on computers somehow extinguishes the judicial findings of "particularity" and the probable cause that justified the warrant in the first place. According to the Court, the Fourth Amendment places just two basic limitations on executive branch officers who seek authority to: (1) search places, where a person has a reasonable expectation of privacy, and (2) seize items believed to be evidence of a crime the officers are investigating.

That is, the *affidavit* of the executive branch officers seeking the warrant must convince the judge through facts and circumstances set out in the affidavit that it is "fairly probable" that evidence of the crime the officers are investigating will be found in each place the officers are asking to search. And, the *search warrant*, itself, must "particularly" describe both the place the officers want to search and the items the officers want to seize. That is all.

Probable Cause – Judges do not have the power to "reject computer warrants" because, as Professor Ohm seems to argue, the volume of non-relevant information likely to be commingled with the evidence of the crime is so vast that it somehow extinguishes probable cause. Rule 41 (c) (1) of the Vermont Rules of Criminal Procedure says that if a judge is satisfied that an officer's affidavit demonstrates there is probable cause to believe that evidence of the crime identified in the warrant will be found in the place identified in the warrant, then, the judge "shall" issue the warrant. Likewise, Rule 41 (d) (1) of the Federal

Rules of Criminal Procedure says the judge "must issue" a warrant on a showing of probable cause. There is no provision in either rule that allows the judge to ignore the fact there is a fair probability that there is evidence of a crime on a computer (or anywhere else) simply because the evidence of a crime is commingled with vast amounts of non-relevant information.

Particularity – Judges also lack the power to add *CDT II* – inspired conditions in an effort to cure what Professor Ohms refers to as "the intractable failure of particularity." Once the judge reviewing a computer warrant (or any other warrant) has made a finding of probable cause, s/he has the duty, and authority, to make sure the warrant "particularly describes:" (1) the location of the computer to be searched and (2) the evidence of the particular crime(s) the case investigators have established probable cause to search for and seize:

> "The Fourth Amendment, however, does not set forth some general "particularity requirement." It specifies only two matters that must be "particularly describ[ed]" in the warrant: "the place to be searched" and "the persons or things to be seized." We have previously rejected efforts to expand the scope of this provision to embrace unenumerated matters." *US v. Grubbs*, 547 US 90, 97 (2006)

THERE IS NO LEGAL BASIS FOR CONDITION 1

It is axiomatic that a court must have a legal basis for its decisions. There is also no question that evidence which tends to prove, or disprove, "any fact of consequence"[49] in a trial, or hearing – is the lifeblood of our justice system. Federal and state law says that *"all relevant evidence is admissible"* unless its admissibility is limited by the U.S. Constitution, the relevant state constitution, statute or other court rules.[50] *But, there is no rule – constitutional, statutory, or evidentiary – that authorizes a judge to dictate, as a condition to granting a computer warrant that all evidence obtained through the plain view doctrine during execution of that warrant, shall be inadmissible, now, and forever more, regardless of whether of this evidence has been obtained legally.*

The only possible basis for a rule requiring exclusion of all digital evidence obtained under the plain view doctrine is the so-called "exclusionary rule" that prevents the prosecution from using evidence that has been obtained illegally in its "direct case" in any criminal trial. No version of the "exclusionary rule" authorizes suppression of evidence before it has been gathered, or even discovered.

The US Supreme Court adopted the "exclusionary rule" for use in federal courts nearly one hundred years ago[51] to *deter* law enforcement officers from violating the U.S. Constitution when they gathered evidence and to *preserve* public

confidence in the integrity of the judiciary by insuring that evidence that was obtained in violation of the Constitution was not used to convict people in our courts. The exclusionary rule has evolved to authorize both federal and state[52] trial judges to prohibit the prosecution from introducing evidence at trial that might otherwise be used to convict a defendant because the government obtained the evidence illegally.

In other words, the evidence is "suppressed" because the prosecution would not have the evidence "but for" the illegal actions of the officers who obtained the evidence (a search that violates the Fourth Amendment for example).[53]

The U.S. Supreme Court has warned that suppression of evidence should be a "last resort" not a "first impulse"[54] and that those seeking to apply the exclusionary rule face a "high obstacle" because suppression of evidence exacts a "costly toll" on "truth-seeking and law enforcement[55]." At the very least, according to the Court, the judge ordering suppression must not suppress evidence unless there has been some misconduct by law enforcement officers in obtaining this evidence. That is, s/he must be satisfied that the evidence that is to be suppressed would not have been discovered "but for" some misconduct by officers who gathered the evidence[56].

Yet, Condition 1 requires "no fault" suppression. Under Condition 1, evidence of a crime that is seized under the plain view doctrine during execution of a computer warrant may never be used. The suppression of this evidence is not based on any evidence that officers have violated the law. Instead, it is based on a presumption that officers, who are trusted to act lawfully in executing any other type of warrant, *will violate the law* when they execute a computer search warrant.

"TRADITIONAL REMEDIES" DO WORK IN COMPUTER CASES

Finally, while there are bound to be isolated instances of police misconduct in computer search cases, there is no need to preemptively exclude an entire class of evidence in anticipation of them. There is good reason to believe that what Chief Judge Woodcock referred to as "traditional remedies" will be adequate to address these individual cases once there is evidence that they *have taken place.*

The potential for abusing the plain view doctrine existed well before computer searches. Officers with a warrant to search for small items that could be hidden virtually anywhere in a home (e.g., illegal drugs) could use the warrant as a pretext to search for evidence for which they did not have probable cause. They could go through every inch of the home under the authority of the "drug warrant;" but, with the intent to look for evidence of other crimes for which they did not have probable cause and then seize this "extra-warrant" evidence when it came into "plain view."

For decades, courts in the United States have dealt with allegations of such police misconduct the same way they dealt with all other allegations of Fourth Amendment violations. They do not order general exclusion of an entire class of evidence *before* it is even discovered as Condition 1 requires. Instead, they address specific claims of misconduct related to a specific search *after that search* has been completed. They routinely rule on these specific claims at hearings on motions to return property, or motions to suppress evidence[57].

These remedies worked well in the CDT case, itself. And defense experts have had little difficulty using metadata to convince judges "after the fact" that government agents had decrypted, searched and seized files that were outside the scope of the computer warrants.[58] There is simply no evidence that these "traditional remedies" will not continue to work in computer searches.

"**STEP AWAY FROM THE COMPUTER**!" – **JUDGES CLAIM THE RIGHT TO BAR POLICE** "**CASE INVESTIGATORS**" **FROM ANY INVOLVEMENT IN CONDUCTING COMPUTER SEARCHES**

CDT Condition 2 is prompted by the same presumption as CDT II Condition 1 – law enforcement "investigators" cannot be trusted to comply with the Fourth Amendment in executing computer searches. It provides:

> "2. Segregation and redaction must be either done by specialized personnel or an independent third party. If the segregation is to be done by government computer personnel, it must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.[59]"

The Vermont version of *CDT* Condition 2 breaks the Condition into three parts[60]; but, it says essentially the same thing. "State investigators" (case investigators) and "prosecutors," those who know the most about the crime that prompted the search of the computer, cannot be involved in the search of the computer. Moreover, they will have *no say* in what digital evidence is ultimately determined to be relevant to *their investigation*. Investigators must leave that determination to court-approved computer forensic experts who know nothing about case at the outset and are barred from communicating with investigators while these independent experts conduct the search.

Federal law and Vermont state law generally require law enforcement officers to execute search warrants.[61] Usually the case investigator, the law enforcement officer who is investigating the crime identified in the warrant, is directly involved in the execution of the warrant. That is no longer the case for computer warrants. The effect of condition 2 is to require law enforcement officers to use a process for searching a suspect's computer that up until now has been reserved

for the rare situations when information on the suspect's computer is believed to be protected by attorney-client privilege[62]. Requiring use of this process in *all computer* searches will *not limit the scope* of computer searches; but, it will significantly undermine the effectiveness of these searches.

TWO BROAD CATEGORIES OF COMPUTER SEARCHES

For purpose of discussion here, there are two broad categories of computer searches – (1) searches of computers controlled by so-called "disinterested third parties" who have no involvement in the crime described in the warrant other than the fact that evidence of that crime is probably stored on their computers (e.g., internet service providers, laboratories, physician's offices, etc.) and (2) searches of computers used by those *suspected* of the crime identified in the warrant.

There is seldom a good reason for case investigators to be directly involved in conducting searches of computers in Category 1. On the other hand, there is almost always a good reason for investigators to be directly involved in conducting searches in Category 2 – computers *used* by suspects.

SEARCHING COMPUTERS CONTROLLED BY "DISINTERESTED THIRD PARTIES"

There are two common circumstances where the need to protect privacy rights of those who are not suspects in a criminal investigation makes it reasonable to have the computer search conducted by third party experts who are not involved in law enforcement.

First, under the Stored Communications Act, state and federal case investigators routinely serve search warrants on providers of electronic communications services (ECS)[63] and remote computing services (RCS)[64] to obtain "content information" that is relevant to crimes identified in the warrant. Employees of the ECS or RCS are legally authorized *to execute these search warrants* without law enforcement officers being present.[65]

Second, third party privacy concerns often make it more reasonable to use a *subpoena* in place of a search warrant. Evidence of a crime is often located on computers owned and controlled by persons or entities (e.g., laboratories, hospitals, "professionals" such as physician's offices) that otherwise have no relationship to the crime under investigation. In such cases, it usually makes sense to attempt to obtain this information by serving a subpoena rather than executing a search warrant.

For instance, U.S. Department of Justice Guidelines[66] (guidelines), require case investigators to use subpoenas when "documentary material" (including

computer files) that is the target of the search is commingled with other, non-relevant information, that is held by "disinterested third parties." i.e., those who are either not suspects in the crime under investigation, or unrelated to suspects. These guidelines cite the need to protect "privacy interests" in situations which are a core concern in computer searches – situations where execution of a search warrant "may require examination of private papers within the scope of the warrant, but not themselves subject to seizure." Using a subpoena, rather than a search warrant[67], gives the "disinterested third party" the opportunity to conduct the search of its own records.

These guidelines can accommodate privacy concerns without jeopardizing effective law enforcement. There is no reason to believe disinterested third parties will destroy evidence of a crime that happens to be on their computers. Since they know their computer systems best, it makes sense for them to search their own computers, after consulting with case investigators who have served them with a subpoena.

SEARCHING COMPUTERS *USED* BY THOSE SUSPECTED OF THE CRIMES IDENTIFIED IN THE WARRANT

However, the majority of computer warrants in Vermont involve searches of computers used by the person suspected of the crime identified in the warrant. The suspect is not "disinterested." He may be reasonably expected to hide and, if given the opportunity, destroy evidence of his crime. Plainly, the suspect cannot search his own computer.

Who then should conduct the search of the suspect's computer? The obvious choice is the case investigator – the officer investigating the case that prompted the warrant. But, on rare occasions,[68] evidence that is subject to seizure under a search warrant is commingled with information that may be protected by attorney-client privilege. On those occasions, independent third parties must take the place of case investigators in conducting the search.

Assume, for instance, it is likely that those executing the warrant will encounter confidential communications (e.g., emails[69]) between the person who is suspected of the crime identified in the warrant and his attorney. Officers investigating the underlying crime are prohibited from involvement in the search. This is because the law prohibits law enforcement officers, in particular, from viewing this highly confidential information. Officers must wait until an independent legal expert who is not involved in the underlying investigation, typically either an outside legal expert ("special master") or a government "taint attorney", reviews the information and separates information that is protected by the privilege from information that is not[70]. This independent expert is, in turn, barred from communicating with case investigators. This serves to eliminate any perception that privileged information is being exploited by these investigators

to fortify their case against the client/suspect.

THERE IS NO LEGAL BASIS FOR TREATING ALL SEARCHES OF A SUSPECT'S COMPUTER AS THOUGH THE ATTORNEY- CLIENT PRIVILEGE APPLIES

Unfortunately, Conditions 2 engrafts a process onto computer that treats *all the information* on *every suspect's* computer as though it is protected by attorney-client privilege. A process that was used once or twice a decade in Vermont, will, instead, be used once or twice a week. Independent experts, not case investigators, will *conduct all searches* of a suspect's computer despite the fact that virtually all of the information that is subject to these searches: (1) is *not protected by privilege* and (2) *is lawfully subject to review* by law enforcement case investigators.

Unlike "taint attorneys" who begin well-prepared to answer the legal question of whether information is covered by the attorney-client privilege; the independent experts conducting the computer searches will be ill-prepared to identify information that "relates to" the crime identified in the warrant. This is because: (1) they are required to start with no knowledge of the underlying investigation and (2) they are prohibited from communicating with the case investigators who could provide this knowledge. Whether information "relates to" the crimes identified in the warrant is largely a question of fact, not law. Under the terms of Conditions 2, the computer search expert is deprived of many of these facts.

CONDITION 2 – ADDED EXPENSE, UNNECESSARY DELAY AND UNFOCUSED SEARCHES

The goal in executing computer warrants (or any other search warrant) is to search for, and seize, relevant evidence – evidence that tends to prove, or disprove, crimes that are identified in the warrant - as quickly as possible.

Case investigators ("agents involved in the investigation") know more about what information is likely to be relevant to the case than anyone else. For example, they know: the chronology of events in the crime, locations, identities of witnesses, relative importance of witnesses, relationships between witnesses, circumstances of witness statements, credibility of witnesses, reliability of witness statements, code words, nicknames, etc. Much of this information may not even be included in the warrant affidavit – a document that is designed to cite facts and circumstances that "establish probable cause" as concisely as possible. Knowledge of this information is undeniably helpful in identifying information that is relevant under the warrant. Yet, the primary purpose of Condition 2 is to *prevent the case investigators* from having any involvement in

the search, or seizure of this evidence in any case, including searches of computers used by a suspect. They will play no part in deciding what digital evidence is relevant to their investigation.

Again, this practice may be legally required in the rare cases where evidence of a crime is likely to be commingled with information protected by attorney-client privilege. But, there is no legal basis for it in the overwhelming majority of computer search cases. Under Condition 2, though, officers involved in any criminal investigation, including rapidly developing investigations involving violent crimes such as murder, attempted murder, sexual assault etc., will have to promise, as a condition for obtaining a computer warrant, to stand aside and wait for an independent expert to select the digital evidence these case investigators may use.

This process will be very *expensive*. As Judge Consuelo Callahan, one of the *CDT II* judges who concurred, in part, and dissented, in part, put it:

> With respect to using an in-house computer specialist to segregate data, the majority's guideline essentially requires that law enforcement agencies keep a "walled-off," non-investigatory computer specialist on staff for use in searches of digital evidence. To comply, an agency would have to expand its personnel, likely at a significant cost, to include both computer specialists who could segregate data and forensic computer specialists who could assist in the subsequent investigation. The alternative would be to use an independent third party consultant, which no doubt carries its own significant expense. Both of these options would force law enforcement agencies to incur great expense, perhaps a crushing expense for smaller police departments that already face tremendous budget pressures."[71]

These conditions will *delay* investigations. Some of these delays may endanger the public – as, for instance, when officers investigating a recent homicide are required to step aside, say nothing, and wait for an independent expert, who knows nothing about their investigation, try to "get up to speed" on their investigation before searching a murder suspect's computer and selecting the evidence the investigating officers will then be allowed to use in continuing their investigation.

There will always be delay – even in straightforward cases like the identity theft case that brought these issues to the Vermont Supreme Court. The court-approved expert, who must at least have a rudimentary knowledge of the crime of identity theft, and its essential elements, will still have to be assigned (or retained[72]), and given time to review the affidavit and warrant to assess what digital evidence might "relate to" the crime identified in the warrant. Then the

independent expert will conduct the search and "segregate" the evidence that s/he *alone* believes is relevant to the crime(s) identified in the warrant. Finally, the independent expert will provide the selected evidence to the case investigator without discussion of any other digital information the expert may have found on the computer.

Delays in cases involving complex transactions and relationships can be absurdly long. In one case where a judge did require the independent expert ("special master") to: (1) filter evidence covered under the attorney-client privilege and (2) decide what digital evidence was relevant to the crimes listed under the search warrant, the trial in the case was delayed for at least *two and one half years.* [73] Delays resulting from review by a special master can "effectively deprive the government of any access to any of the seized information."[74]

Independent experts do not have to mean delay. In fact, prior to Condition 2, they meant greater speed and efficiency. Specially-trained law enforcement officers who are experts in searching computers are an important asset to criminal investigations. These officers *work with* case investigators. The fact that the expert starts with little knowledge of the case does not result in delay because the expert routinely consults with case investigators to decide what digital information is relevant to the case. Their skill in searching computers speeds the process. Their ability to consult with case investigators enables them to narrow the scope of the search, and sharpen their focus on only the most relevant, case specific information, thereby further speeding the process.

This can no longer happen under Conditions 2 because the expert in searching computers is prohibited from consulting with the case investigator. The expert must remain behind a "firewall." Since the expert cannot discuss the case with the investigating officer while conducting the search, the expert will have to rely on the information in the affidavit(s) and the search warrants, itself, to determine what digital evidence the expert will seize and eventually give to investigators. Because the affidavit and warrant will not provide the expert with all of the facts and circumstances developed during the investigation, the search will be less efficient and less effective.

Again, the affidavit supporting the warrant in the case before the Vermont Supreme Court is a good example. The case involves investigations of identity theft by police agencies in two states.[75] Yet, aside from the names of investigators, the affidavit, which easily establishes probable cause, contains only three names. One was the name of the 84-year-old New York resident who was the victim of the attempted ID theft. The second was the name of the owner of the property at an address in Vermont – an address that a bogus application for a credit card had falsely identified as the victim's address. The third was the name of the innocent subscriber assigned to the IP address that was used to submit the bogus application. This person's "open" wireless network was

evidently used by the thief.[76]

Although there were multiple attempts to obtain different credit cards through false representations, the affidavit contains details of just one attempt[77]. The case investigator would have more names and many more details. Because of Condition 2, an independent expert "segregating" digital evidence found on the suspect's computer will not have this additional information. The expert, who must remain behind a "firewall," barred from communicating with case investigators, will not have the names of contacts and details of the attempts to obtain other credit cards.

This, in turn, creates a substantial likelihood that the computer search expert will not have key words, such as the names of other banks and credit card companies he needs to identify digital evidence that "relates to" attempts to steal the victim's identity. In addition, the expert will not have the names of friends and associates of the victim who may have knowledge of, or access to, the victim's identification information and who may have intentionally, or unwittingly, given this information to the thief. Again, because he does not know the relevance of these names, he will not search for them, or recognize their significance if he happens upon them. It is important to point out that the expert will also not have names of others who had access to the computer, which the would-be-thief apparently used to make the bogus application. The expert will not even know the names of others who had access to the open wireless network used in the attempt.

In short, the independent expert is likely to miss relevant evidence – evidence that tends to prove, or disprove, the suspect's guilt.

Computer searches are likely to be broader, and, in that sense, more intrusive. This is because it is more likely that the independent expert will pursue leads (and review files) unnecessarily. For instance, in the identify theft case before the Vermont Supreme Court, the expert is likely to come across digital information on the suspect's computer that appears to be relevant because it deals with credit or financial transactions. Some will be relevant. Some will not. The independent expert will not be able to contact the investigator, who would have sufficient knowledge of relevant financial transaction to advise the expert on whether particular transactions "relate to" the underlying crime. Without this advice, the expert is likely to unnecessarily investigate transactions that have nothing to do with the crime identified in the warrant.

CONDITION 2 DOES NOT LIMIT GOVERNMENT "DISCRETION"

James Saylor, another commentator who supports *CDT* conditions, argues in the Fordham Law Review that conditions such as Conditions 2 are *"perhaps the most important"* of the *CDT II* –inspired conditions[78] because they will deprive "the government" of the "discretion" that enables "the government" to conduct "dragnet searches."[79]

Of course "the government" doesn't search computers. It searches computers through people who work as its agents. The independent expert/ "special master" who conducts the search will be no less a "government agent" than the case investigator, or any other law enforcement officer, who executes a search warrant. The special master's authority to conduct the search will be derived from the very warrant that the case investigator obtained – but was barred by Conditions 2 from executing. His/her goal in conducting the search will be same as that of the case investigator – to search for, and seize, evidence that tends to prove, or disprove, crimes that are identified in the warrant – as quickly as possible.

The fact is Condition 2 does nothing to limit "discretion" or the potential for abuse of discretion. It simply substitutes "government agents" (independent experts) who know nothing about the case for "government agents" (case investigators) who do know something about the case. *Unless judges come to the unlikely conclusion that all computers are constitutionally immune from search because of the potential for abuse, there is going to be someone "from the government" who will be conducting computer searches.*

CONDITION 1 MAKES CONDITION 2 UNNECESSARY

Condition 2 does have the unwarranted effect of treating all evidence that is subject to computer searches as though this evidence is covered by the attorney-client privilege. But, concern for attorney-client privilege is not what prompted Condition 2. Ultimately, the concern that prompted Condition 2 is the same concern that prompted Condition 1. It is the belief that case investigators are more likely to deliberately violate the Fourth Amendment and turn computer searches into "general warrants" than other "government agents." Mr. Saylor put it this way:

> Appointing a special master assures that any authority to view files potentially outside the scope of the warrant is granted to an official unconnected to the investigation and uninterested in "extend [ing] a general exploratory search from one object to another until something incriminating at last emerges."[80]

There is still no evidence to support this concern. But, the fact is, even if such evidence existed, the existence of Condition 1 would still make Condition 2 unnecessary.

Condition 1 requires the prosecution to pledge, as a condition of obtaining the computer warrant, to never use digital evidence seized under the plain view doctrine while executing the warrant. This eliminates the incentive for *any* government agent, including case investigators, to rummage for evidence of crimes for which s/he knows there is no probable cause. There is no incentive to

engage in an unlawful "general exploratory search" and seize evidence under the plain view doctrine because government agents (case investigators) have already agreed as Condition 1 for obtaining the warrant that they will never use such evidence.

Condition 1 *is "unwise."* But, it is also *easy to enforce.* Even if an investigator were tempted to violate Condition 1, s/he would not be successful. Prosecutors must always prove of the source of a piece of evidence in order to authenticate and admit it at trial. Assume case investigators have agreed to Condition 1 in order to obtain a computer warrant to search for evidence of *identity theft.* It would be virtually impossible to later authenticate and admit evidence of another crime e.g., evidence of *possession of child pornography* that had been seized under the plain view doctrine during execution of the *identity theft* warrant. It would be obvious to the judge and defense counsel during the authentication process that prosecution has violated Condition 1 by seeking to admit evidence of *possession of child pornography* that was obtained during execution of a warrant that authorized government agents to search solely for evidence of *identity theft.*

Condition 2 prohibits investigators from taking any role in executing the computer warrants they have obtained. It is based on the unwarranted presumption that investigators are more likely than other government agents to exploit the plain view doctrine. Condition 2 is unnecessary because Condition 1 already eliminates both the incentive, and the ability, to exploit this doctrine. In fact, Condition 2 is more than unnecessary, it is "worse than useless." It prohibits investigators from playing any role in reviewing evidence seized under the warrant they have obtained, and deciding what pieces of digital evidence are relevant to the crimes they are investigating. In doing so, Condition 2 increases expense, delay and the likelihood that relevant evidence will be overlooked, while at the same time adding nothing to the protection from potential privacy violations that Condition 1 already provides.

---

[1] Robert V. Simpson, Jr., graduated from Colgate University (BA, 1967), Vermont Law School (JD, 1978) and served as a prosecutor in Chittenden County (Vermont) between 1979 and 81 and again between 1994 and 2006.

[2] *In Re Appeal of Application for Search Warrant,* No. 2010-479 (S. Ct. Vt. Filed December 29, 2010)

[3] The prosecutors' first argument is that Vermont judges lack legal authority to impose these preconditions. This dispute over whether judges have the *legal authority* to impose these restrictive preconditions has become, in part, a battle by proxy between law professors. Prosecutors rely on the analysis of George

Washington University Law Professor, Orin Kerr, who argues that judges do not have legal authority to impose conditions on how officers will execute search warrants. Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 Va. L. Rev. 1241 (2010) Two national organizations, the Criminal Law Reform Project of the ACLU Foundation and the Electronic Frontier Foundation (EFF) responded to the prosecutors' reliance on Professor Kerr by countering with the March 2011 reply to Professor Kerr by Professor Paul Ohm. Brief of ACLU and EFF, filed in Docket No. 2010-479 on June 17, 2011 at 15. Professor Ohm contends these conditions are not only lawful, but necessary. Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 Va. L. Rev. 1, 4 (March, 2011)

[4] The Vermont conditions are:

> 1. As a condition for receiving a search warrant to search the subject computer, the State cannot rely upon the "plain view doctrine" to seize any electronic records other than those authorized by this warrant. That is, any digital evidence relating to criminal matters other than the identity theft offenses, may not be seized, copied, or used in any criminal investigation or prosecution of any person.
> 2. Inspection and investigation of the subject computer must be done by either an independent third party or specially trained computer personnel who are not involved in the investigation while staying behind a firewall, that is, in the absence of other agents of the State, and subject to a ban on copying or communicating to any person or the State any information found on the subject computer other than digital evidence relating to identity theft offenses.
> 3. Any digital evidence relating to the offenses must be segregated and redacted before it is provided to the State, no matter how intermingled it is.
> 4. If the segregation is performed by State computer personnel, it is a condition of this warrant that the computer personnel will not disclose to the State investigators or prosecutors any information other than that which is the target of the warrant, that is, digital evidence of the identity theft offenses.
> 5. The search protocol employed must be designed to uncover only the information for which the State has probable cause, that is the aforesaid alleged offenses, and only that digital evidence may be provided to the State. Techniques to focus the search should include but are not limited to, specific time periods relevant to the alleged criminal activity, key word searches, and limiting the search to specific file types.
> 6. The government has at its disposal sophisticated hashing tools that allow identification of well-known illegal files (such as child pornography) that are not at issue in this case. These and similar search tools may not be used without specific authorization by the court.

> 7. Information relevant to the targeted alleged activities may be copied to other media to provide to State agents. No other digital evidence may be so copied.
> 8. The government must return non-responsive data, keeping the court informed about when it has done so and what it has kept.
> 9. Any remaining copies of the electronic data must be destroyed absent specific judicial authorization to do otherwise.
> 10. Within the time specified in the warrant, the State must provide the issuing officer with a return disclosing precisely what data it has obtained as a consequence of the search, and what data it has returned to the party from whom it was seized. The return must include a sworn certificate that the government has destroyed or returned all copies of data that it is not entitled to keep.

In re: Application for Search Warrant Eric Gulfield Computer, Chittenden Superior Court , Amended Order at 1 (Dec. 22, 2010) Printed Case (PC) 3-4

[5] Judge Michael Kupersmith is a respected trial judge with well-over twenty years of experience in Vermont's Criminal Division.

[6] In re: Application for Search Warrant Eric Gulfield Computer, Chittenden Superior Court, Amended Order at 1 (Dec. 22, 2010) Printed Case (PC) 3-4 "The application to search the computer belonging to Eric Gulfield is *granted* subject to the conditions listed herein. In setting these conditions, the Court has been guided by *United States v. Comprehensive Drug Testing, Inc.,* 579 F.3d 989 9th Cir. (2009)."

[7] The 9th Circuit is the largest Federal Circuit Court of Appeals in the United States. It covers federal courts in Arizona, California, Nevada, Montana, Oregon, Idaho, Washington, Alaska and Hawaii as well as Guam and the Northern Marianna Islands.

[8] *United States v. Comprehensive Drug Testing, Inc.*,579 F.3d 989 (9th Cir.2009)

[9] *CDT II*, 579 F.3d 989, 1000

[10] *Id*

[11] Chief Judge Kozinski summarized the "guidance" that magistrates "must be vigilant" in observing:

> 1. Magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.
> 2. Segregation and redaction must be either done by specialized personnel or an independent third party.

> If the segregation is to be done by government computer personnel, it must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.
> 3. Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora.
> 4. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.
> 5. The government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.

United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1006 (9th Cir.2009) (internal citations omitted)

[12] *US v. Comprehensive Drug Testing Inc.,* 621 F3d 1162,1176 (9th Cir 2010) (*CDT III*)

[13] *CDT III* at 1180

[14] *CDT III* at 1178

[15] In the Matter of the United States Of America's Application For A Search Warrant To Seize And Search Electronic Devices From Edward Cunnius, 770 F. Supp. 2d 1138, 1139 (W.D. Washington, 2011)

[16] According to Detective Lt. Kris Carlson of the Burlington (Vermont) Police Department, an officer with long experience as a computer forensic investigator, Vermont police officers have specific objections to nearly all of the *CDT* conditions. But their overriding general objection is that, although they well understand that computers can contain huge amounts of private information, they see no reasonable justification for the imposition of vastly greater restrictions on searches of computers than restrictions on searches of homes, which are generally considered the most private of private places. Recorded interview with Detective Lt. Kris Carlson, Director of Vermont's Internet Crimes Against Children (ICAC) Task Force in Burlington, Vermont on July 19, 2011

[17] Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges,* 97 Va. L. Rev. 1, 3, 8 (March, 2011)

[18] 97 Va. L. Rev. 8

[19] Bryan Weir, *It's (Not So) Plain to See: The Circuit Split on the Plain View Doctrine in Digital Searches*, 21 Geo. Mason U. Civ. Rts. L. J. 83, 113 (Fall 2010); James Saylor, *Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches,* 79 Fordham Law Review 2809 (May, 2011); James Stinsman, *Computers and Searches, Rethinking the Applicability of the Plain View Doctrine*, 83 Temple Law Review 1097, 1120 (Summer 2011) and Matthew Dodovich, *The Plain View Doctrine Strikes Out In Digital File Searches,* 6 ISLP 659, 691 (Summer, 2011)

[20] E.g., summaries of statements from customers and neighbors

[21] The U.S. Supreme Court has said that "probable cause" means that there is a "fair probability" that contraband or evidence of a crime is at a particular place. *Illinois v. Gates,* 462 US 213, 238 (1983)

[22] The officer must also prepare an application but that document merely gives the judge an outline of the substantive information developed in the warrant and the supporting affidavit.

[23] The judge, in turn, "must" grant the warrant if there is probable cause to believe that the evidence of the crime identified in the warrant is located at the place identified in the warrant. The applicable Court Rules are Fed. R. Crim. P 41 (d) (1) which says:

> (1) *In General.* After receiving an affidavit or other information, a magistrate judge – or if authorized by Rule 41(b), a judge of a state court of record – must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device;
>
> and Vt. R. Crim P 41 (c) which says
>
> (1) *Probable Cause.* A judicial officer shall issue the warrant if the judicial officer is satisfied that there is probable cause to believe that grounds for the application exist based upon an affidavit or affidavits or sworn testimony or both."

[24] The warrant which is now before the Vermont Supreme Court says:

> "To: Det. Michael Warren and any Vermont Law Enforcement Officer
> **You are hereby commanded to search:"** (emphasis in the original)

[25] "The application to search the computer belonging to E.G., is *granted* subject to the conditions listed herein. In setting these conditions, the Court has been guided by *United States v. Comprehensive Drug Testing, Inc.,* 579 F.3d 989 9th Cir. 2009)." Amended Order, In re: Application for Search Warrant E_G_ Computer, December 22, 2010 at 3

[26] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[27] *Horton v. California,* 496 US 128 (1990)

[28] Crimes Act 1914 Section 3F - http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/s3f.html

[29] "The problem can be stated very simply: There is no way to be sure exactly what an electronic file contains without somehow examining its contents either by opening it or looking, using specialized forensic software, keyword searching or some other such technique. But electronic files are generally found on media that also contain thousands or millions of other files among which the sought-after data may be stored or concealed. By necessity, government efforts to locate particular files will require examining a great many other files to exclude the possibility that the sought-after data are concealed there." *CDT II*, 579 F3d at 1004.

[30] See, Orin S. Kerr, *Searches and Seizures in a Digital World,* 119 Harv. L .Rev. 531, 568-71 (2005)

[31] "Thus, the scope of a lawful search is 'defined by the object of the search and the places in which there is probable cause to believe it may be found." *Maryland v. Garrison*, 480 US 79, 84(1987) (quoting *US v. Ross*, 456 US 798, 824 (1982) The scope of the search in the hypothetical is limited by the "object" of the search – evidence of the crime of sale of marijuana, the crime identified in the warrant and a crime for which the officer had probable cause. The officer exceeded the scope of the warrant because he was looking for evidence of the crime of sexual exploitation of a child – a crime that was not identified in the warrant, and a crime for which he did not have probable cause.

[32] "It is, of course, an essential predicate to any valid warrantless seizure of incriminating evidence that the officer did not violate the Fourth Amendment in arriving at the place from which the evidence could be plainly viewed." *Horton*, 496 US at 136.

[33] 579 F3d at 997-999, 1005

[34] 579 F3d 998

[35] *Id*

[36] 579 F3d 1006

[37] *U.S. v. Farlow,* 2009 WL 4728690 (D. Me. 2009, slip opinion p. 6 fn3)

[38] *In Re Appeal of Application for Search Warrant,* No. 2010-479 (S. Ct. Vt. Filed December 29, 2010), affidavit of Detective Michael Warren in support of application for search warrant, Printed Case (PC) 8-9

[39] The investigator, Detective Warren, does have training and experience in computer forensic investigations. *Id.* 7

[40] Vermont officer/examiners are taught to confine the scope of their searches to the evidence delineated in the search warrant. If they do open a file that reveals evidence of another crime "in plain view," they apply for another warrant. Interview with Detective Lt. Kris Carlson, Director of Vermont's Internet Crimes Against Children (ICAC) Task Force in Burlington, Vermont on July 19, 2011

[41] 97 Va. L. Rev. 5

[42] *Id*

[43] Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges,* 97 Va. L. Rev. 11 (March, 2011)

[44] 97 Va. L. Rev. 4

[45] Whether the place to searched, is a car, a home or a computer, the officers always "seize" the place to be searched first in the sense that they take control of that place before they begin searching through non-incriminating objects and information for evidence of the crime identified in the warrant. The big difference in computer searches is that the search of the copied hard drive usually takes places offsite.

[46] 97 Va. L. Rev. 7

[47] 97 Va. L. Rev. 8

[48] *US v. Upham,* 168 F3d 532, 535 (1st Cir., 1999)

[49] Fed. R. Evid. 401; Vt. R. Evid. 401

[50] Fed. R. Evid. 402; Vt. R. Evid. 402

[51] *Weeks v. US,* 232 US 383 (1918)

[52] *Mapp v. Ohio*, 367 US 343 (1961)

[53] *US v. Herring*, 555 US 135, 141 (2009)

[54] *Hudson v.* Michigan, 547 US 586, 591 (2006)

[55] *Id.*

[56] "Our cases show but-for causality is only a necessary, not sufficient, condition for suppression." 547 US at 592

[57] According to one source, there are roughly 175,000 "suppression hearings" held in our courts in the U.S. each year on Fourth Amendment issues alone. Joel Samaha, *Criminal Procedure*, 7th edition 361 (2008)

[58] *U.S. v. Kim*, 677 F. Supp. 2d 930, 950(S.D. Texas, 2009)

[59] 579 F3d at 1006

[60] 2. Inspection and investigation of the subject computer must be done by either an independent third party or specially trained computer personnel who are not involved in the investigation while staying behind a firewall, that is, in the absence of other agents of the State, and subject to a ban on copying or communicating to any person or the State any information found on the subject computer other than digital evidence relating to identity theft offenses.
3. Any digital evidence relating to the offenses must be segregated and redacted before it is provided to the State, no matter how intermingled it is.
4. If the segregation is performed by State computer personnel, it is a condition of this warrant that the computer personnel will not disclose to the State investigators or prosecutors any information other than that which is the target of the warrant, that is, digital evidence of the identity theft offenses.

[61] The federal law says: "A search warrant may in all cases be served by any of the officers mentioned in its direction or by an officer authorized by law to serve such warrant, but by no other person, except in aid of the officer on his requiring it, he being present and acting in its execution." 18 USC 3105

Vermont Rule of Criminal Procedure 41 (c) (5) likewise says the warrant must be executed by a law enforcement officer: ". . . The warrant shall be directed to a law enforcement officer of the state of Vermont authorized to enforce or assist in enforcing any law thereof. The warrant shall command the officer to search the person or place named for the property or other object specified and seize the property or object and, if appropriate, the person specified."

[62] Vermont Rule of Evidence 502; Federal Rule of Evidence 502

[63] E.g., Comcast, Yahoo!

[64] E.g., businesses that store and process electronic billing information for physicians

[65] 18 USC 2703 (g)

[66] U.S. Attorneys Criminal Resource Manual, part 59-Guidelines on Methods of Obtaining Documentary Materials Held by Third Parties, 28 C.F.R. Part 59, § 59.1

[67] Investigators may proceed by search warrant – but only when using a subpoena would "substantially jeopardize the investigation. *Id.*

[68] I worked for roughly fifteen years as a prosecutor in Vermont. I am aware of only two cases when it was necessary to use an independent third party to execute the search warrant in order to sort out material that was protected by attorney-client privilege. One of the two cases involved a computer warrant. (*U.S. v. Hunter*, fn. 70 – below)

[69] *U.S. v. Taylor*, 764 F. Supp. 2d 230, 232-36 (D. Me. 2011)

[70] *U.S. v. Hunter*, 13 F. Supp. 2d 574 (D. Vt. 1998) involved a computer search warrant of records of an attorney who published a legal newsletter. The search raised both attorney-client privilege issues and Privacy Protection Act questions. The US Attorney for Vermont designated a team consisting of an attorney and officers who were not involved in the criminal investigation ("taint team") to conduct the search and sort out evidence that the investigating officers were authorized to view under the warrant.

[71] *CDT II*, 579 F3d 989, 1013 (Callahan, Circuit Judge, concurring in part, dissenting in part)

[72] Despite the apparent requirements of Rule 41 of the Vermont Rules of Criminal Procedure, Condition 2 does not require the "independent expert" to be a law enforcement officer.

[73] The case is *US v .Abbell*, 914 F. Supp. 519 (S.D. Fla. 1995). The delay is reported in *Black v. US*, 172 FRD 511, 514 n.4 (S.D. Fla. 1997)

[74] 172 FRD 516

[75] New York State Police conducted the initial investigation and then gave information that they had to Burlington, Vermont Police because it appeared the person suspected of the crime lived in Burlington. *In Re Appeal of Application for Search Warrant,* No. 2010-479 (S. Ct. Vt. Filed December 29, 2010) PC 5-11

[76] Id

[77] PC 6-7

[78] *Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches*, 79 Fordham L. Rev. at 2856

[79] 79 Fordham L. Rev. at 2857

[80] *Id.*