

STATE OF NORTH CAROLINA)	
)	
VS.)	AFFIRMATION IN OPPOSITION TO
)	DEFENSE MOTION TO COMPEL
BRADLEY GRAHAM COOPER,)	DISCOVERY
Defendant.)	
)	
-----)	

James R. Durie, being duly sworn, deposes and state:

1. I am a Supervisory Special Agent (SSA) with the Federal Bureau of Investigation (FBI), currently assigned to the Digital Evidence Section (DES), Investigative Analysis Unit (IAU). My previous assignment was to the Digital Evidence Laboratory (accredited by the American Society of Crime Laboratory Directors, Laboratory Accreditation Board (ASCLAD/LAB) under international standards), Computer Analysis Response Team (CART) Operational Support Unit (OSU) at FBI Headquarters in Quantico, Virginia. FBI CART OSU is responsible for overseeing the nationwide operation of the FBI's entire digital evidence forensic laboratory program, including establishing policies, providing technical support, and other leadership and guidance as necessary. As a field operations program manager in CART OSU, I was responsible for establishing and advising on policy guidance.

2. I have a Bachelor of Science degree in Police Science and Law Enforcement from Sam Houston State University and a Juris Doctorate from Southwestern University School of Law. I worked as a technical analyst conducting test and validation research for PC's Limited (now Dell Computers) for approximately two years prior to beginning my federal law enforcement career. I have over twenty-three years experience in federal law enforcement including twelve years with the U.S. Immigration and Naturalization Service. I was employed by the FBI in 1998 and was assigned to work counterterrorism and drug cases prior to my assignment to the FBI's Los Angeles Division's CART squad in 2000.

3. I have ten years experience working in the field of computer forensics. I have completed college courses in computer programming, computer forensics, digital communications, forensic pathology, mathematics, and statistical analysis, as well as approximately 2000 hours in computer forensics training. I was initially certified as a CART Forensic Examiner (Basic Wintel FE Certification) on March 4, 2002. Subsequently, I received my UNIX certification on July 7, 2003, and my Macintosh certification on September 28, 2004. I have served as either a certified CART forensic examiner or a Program Manager managing CART forensic functions continuously from March 4, 2002 until June 6, 2010. I am currently assigned

as the Program Manager for the Investigative Analysis Unit (IAU) managing intrusion and malware analysis for criminal and counter-terrorism investigations. In CART and CART-OSU, I managed field operations, CART Tactical operations, coordinated test and validation of forensic tools used by CART, and provided training to other agencies, foreign governments, and FBI new agents at the FBI Academy. I am an Adjunct Professor at George Mason University, where I teach undergraduate courses in Information Security and Computer Forensics and graduate courses in Computer Forensics.

The Nature of the Defense Request and General Response

4. I have reviewed the relevant portions of the defense motion in this case.
5. I understand that the Defendant has requested the court compel the State of North Carolina and the Federal Bureau of Investigation to provide a copy of the FBI CART policies and procedures for the viewing, extraction or examination of digital data; the FBI's policies on how the analysis of the Macbook Pro computer was examined by a member of the Durham Police Department as opposed to an FBI examiner; and numerous other documents from FBI Special Agent (SA) Johnson pertaining to his examination of the computers in this case, including but not limited to communications logs, examiner bench notes, and all other documents completed or compiled by SA Johnson beyond the

Report of Examination, which was already disclosed.

6. The FBI has always asserted that the documents and materials requested by the defense from the FBI are exempt from discovery pursuant to the "law enforcement sensitive" qualified evidentiary privilege. See In re U.S. Department of Homeland Security, 459 F.3d 565, 569-71 (5th Cir., 2006) (finding that "in today's times the compelled production of government documents could impact highly sensitive matters relating to national security. Therefore, the reasons for recognizing the law enforcement privilege are even more compelling now than when [prior cases in the 5th Circuit] were decided."); Tuite v. Henry, 181 F.R.D. 175, 176-77 (D.D.C. July 31, 1998) (unpublished), aff'd Tuite v. Henry, 203 F.3d 53 (D.C.Cir.1999) ("The federal law enforcement privilege is a qualified privilege designed to prevent disclosure of information that would be contrary to the public interest in the effective functioning of law enforcement. [It] serves to preserve the integrity of law enforcement techniques and confidential sources, protects witnesses and law enforcement personnel, safeguards the privacy of individuals under investigation, and prevents interference with investigations."); United States v. Van Horn, 789 F.2d 1492, 1507-1508 (11th Cir.), cert. den., 479 U.S. 854 (1986) (finding the existence of a qualified government privilege not to disclose sensitive investigative techniques); Dellwood Farms v.

Cargill, Inc., 128 F.3d 1122, 1125 (7th Cir., 1997); In re Dep't of Investigation, 856 F.2d 481, 483-84 (2d Cir., 1988) (stating that the law enforcement privilege exists and prevents the "disclosure of law enforcement techniques and procedures, [preserves] the confidentiality of sources, [protects] witnesses and law enforcement personnel, [safeguards] the privacy of individuals involved in an investigation, and otherwise [prevents] interference with an investigation"); United States v. Winner, 641 F.2d 825, 831 (10th Cir.1981) (stating that the "law enforcement investigative privilege is based primarily on the harm to law enforcement efforts which might arise from public disclosure of investigatory files") (internal quotation marks and ellipse omitted); see also United States v. Harley, 682 F.2d 1018, 1020-21 (D.C.Cir.1982); United States v. Green, 670 F.2d 1148 (D.C.Cir.1981).

7. The FBI routinely asserts this privilege because the CART Standard Operating Procedures (SOP) and other policies sought by the defendant are a step-by-step list of procedures on how the FBI deploys investigational tools in a computer forensics investigation. The examiner's bench notes essentially track the SOPs step-by-step. Given the nature of these materials, a computer savvy defendant, criminal enterprise or foreign power, should they gain access to the notes, could determine the FBI's techniques, procedures and capabilities in this area. This

knowledge could lead to the development and employment of countermeasures to FBI tools and investigative techniques by subjects of investigations and completely disarm law enforcement's ability to obtain forensic data in criminal investigations. This, in turn, could completely prevent the successful prosecution of criminal cases involving digital evidence, including child pornography, computer intrusion, financial fraud, and a variety of white collar crimes.

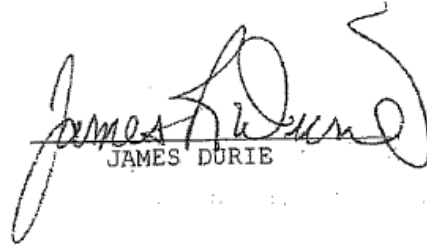
8. Adding to the sensitive nature of the FBI's SOPs and policies in ordinary criminal cases, the same techniques and tools are often used in counterterrorism and counterintelligence investigations. Thus, the compromise of the FBI's investigational tools and methods in a criminal case could have a significant detrimental impact on the national security of the United States.

9. Recognizing that a defendant has the ability to (1) hire a defense expert to perform his own independent examination of the seized materials, and (2) question an FBI CART examiner on cross-examination based on the examiner's report (which has been disclosed) with the advice and assistance of the defense expert, the Federal Rules of Criminal Procedure, Rule 16(a)(2), do not provide for the routine discovery of examiner notes or SOPs (internal government documents made by an agent of the government "in connection with investigating or prosecuting [a]

case," are not subject to discovery.). The same policy reasons are in play in the instant case. Here, the FBI provided to the defense an image copy of the seized computers, and the defendant can hire his own computer forensic defense expert to perform his own independent investigation. If there is an issue of fact between evidence the FBI examiner purports to have recovered and the defense expert's examination, that can be fully explored at trial by the defense under cross-examination of the FBI agent, or through direct examination of his expert. Access to the SOPs and bench notes will not aid in this avenue of approach, as it will be the defense expert's own examination that provides the basis for the defense's questions and evidence.

10. Alternatively, should the court decide production of any of the documentation requested is relevant and material enough to overcome the privilege, we request that release of materials be conducted under strict conditions and only subject to a protective order from the court. Specifically, the conditions should include that any materials disclosed may only be reviewed in FBI space under FBI supervision; that the notes or SOPs not be physically transferred to defense counsel; that they not be photocopied, imaged or duplicated in any fashion (including handwritten or otherwise recorded notes, summaries, or sketches); that defense counsel be prohibited from bringing any devices or materials capable of recording or duplicating the

materials into the review space; and that counsel and any belongings be subject to search both before and after the review session.


JAMES DURIE

Dated: June 10, 2010