15-1815

UNITED STATES COURT OF APPEALS
FOR THE
SECOND CIRCUIT

UNITED STATES OF AMERICA, *Appellee,*

-v.-

ROSS WILLIAM ULBRICHT, *Defendant-Appellant.*

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK

AMICUS CURIAE BRIEF OF THE NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS IN SUPPORT OF DEFENDANT-APPELLANT AND ARGUING REVERSAL

STEVEN R. MORRISON
UNIVERSITY OF NORTH DAKOTA
SCHOOL OF LAW
1526 Robertson Court
Grand Forks, North Dakota 58201
(617) 749-7817

Vice Chair, NACDL Amicus Curiae Committee

JOEL B. RUDIN
LAW OFFICES OF JOEL B. RUDIN, P.C.
600 Fifth Avenue, 10th Floor
New York, NY 10020
(212) 752-7600

Vice Chair, NACDL Amicus Curiae Committee

CORPORATE DISCLOSURE STATEMENT

Amicus curiae National Association of Criminal Defense Lawyers ("NACDL") submits the following corporate disclosure statement, as required by Fed. R. App. P. 26.1 and 29(c): NACDL is a nonprofit corporation organized under the laws of the District of Columbia. It has no parent corporation, and no publicly held corporation owns ten percent or more of its stock.

Dated: January 18, 2016
Grand Forks, North Dakota

Steven R. Morrison
Steven R. Morrison

Attorney for Amicus Curiae National Association of Criminal Defense Lawyers

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Sources **Page(s)**

United States Supreme Court

Second Circuit Court of Appeals

Other Circuit Courts of Appeals

Other Courts

Constitutional Provisions

Rules and Regulations

Other Sources

STATEMENT OF IDENTITY, INTEREST, AND AUTHORITY

Amicus the National Association of Criminal Defense Lawyers ("NACDL") is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct.[1] NACDL was founded in 1958. It has a nationwide membership of approximately 10,000 direct members in 28 countries, and 90 state, provincial, and local affiliate organizations totaling up to 40,000 attorneys. NACDL's members include private criminal defense lawyers, public defenders, military defense counsel, law professors, and judges. NACDL files numerous *amicus* briefs each year in the Supreme Court and other courts seeking to provide *amicus* assistance in cases that present issues of broad importance to criminal defendants, criminal defense lawyers, and the criminal justice system as a whole. In particular, in furtherance of NACDL's mission to safeguard fundamental constitutional rights, the Association frequently appears as *amicus curiae* in cases involving the Fourth Amendment and its state analogues, speaking to the importance of balancing core constitutional search and seizure protections with other societal interests.

[1] Pursuant to Fed. R. App. P. 29(c)(5) and Rule 29.1 of this Court's Local Rules, amicus curiae certify that (1) this brief was authored entirely by counsel for the NACDL, and not by counsel for any party, in whole or part; (2) no party or counsel for any party contributed money to fund preparing or submitting this brief; and (3) apart from the NACDL and its counsel, no other person contributed money to fund preparing or submitting this brief.

The NACDL files this brief in support of appellant Ross William Ulbricht and urges the Court to reverse the District Court decision that denied Ulbricht's motion to suppress. The warrants that provided the authority for law enforcement agents' search and seizure of Ulbricht's laptop computer and his Gmail and Facebook accounts lacked a particularity statement as to the place to be searched and things to be seized. They were, therefore, unconstitutional general warrants.

The issue of particularity arising in this case has obvious ramifications for Ulbricht. This case also reflects ongoing problems with warranting searches of digital data in a way that promotes effective law enforcement while protecting citizens' privacy. While this balance has largely been established as regards searches of physical spaces, such as mail sent through the United States Postal Service, physical papers stored in someone's home, medical records, or books, courts, including this Court, offer very different and conflicting approaches to balancing these interests in the digital context. The NACDL therefore, also asks this Court to address those underlying issues through a comprehensive articulation of core Fourth Amendment concepts, reinterpreted for the digital age.

Pursuant to Fed. R. App. P. 29(a), amicus has sought and obtained consent of all parties to file this brief.

ARGUMENT

I. The warrants issued in this case lacked a limiting statement of particularity and were therefore unconstitutional, violating the original intent of the Fourth Amendment, extant historical and contemporary jurisprudence, and this Court's case law

A. Introduction

Ulbricht argues, under his issue VI.A, that the District Court erred in denying his motions to suppress evidence from his laptop and social media accounts because the warrants authorizing those searches lacked any particularity. (Blue Br. 2, 98-108). We argue that to satisfy the mandates of the Fourth Amendment's particularity requirement, courts must rethink how magistrates draft and issue warrants. This includes paying special attention to pre-search instructions as well as post-search reasonableness analyses. To that end, we proceed in the following manner.

In section B, we discuss the original underpinnings of the Fourth Amendment's particularity requirement, which were greatly informed by the evil of British general warrants and the concomitant need for limiting statements of particularity.

In section C, we trace the development of Fourth Amendment jurisprudence through eras of technological advancement, and show that in each era, courts have been able to reinterpret the application of the Fourth Amendment to meet new realities while remaining faithful to the Amendment's

core purpose: to protect individuals' privacy against undirected and generalized governmental rummaging.

In section D, we discuss the need for a careful assessment of particularity statements in warrants to search digital data. We also discuss why the particularity requirement was not satisfied in Ulbricht's case.

In section E, we discuss the current law on warranted digital searches. In this section, we discuss the issue of particularity and the use of both pre-search instructions, championed by former Ninth Circuit Chief Judge Alex Kozinski, see United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010) [hereinafter CDT], and robust post-search reasonableness inquiries into law enforcement agents' warranted digital searches. Both pre-search instructions and post-search reasonableness inquiries are necessary to ensure the existence and effective operation of limiting statements of particularity.

In section F, we address the warrants that issued in Ulbricht's case and offer provisions that the magistrate should have included that would have supplied the requisite particularity and still ensure effective law enforcement.

B. The Fourth Amendment at its framing: the need for particularity

Fourth Amendment protections played an essential role in the founding of the country, and were meant to provide refuge from the "general warrants" deployed by British authorities during the colonial era, and which spurred the American Revolution itself:

> Our cases have recognized that the Fourth Amendment was the founding generation's response to the reviled "general warrants" and "writs of assistance" of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity. Opposition to such searches was in fact one of the driving forces behind the Revolution itself. In 1761, the patriot James Otis delivered a speech in Boston denouncing the use of writs of assistance. A young John Adams was there, and he would later write that "[e]very man of a crowded audience appeared to me to go away, as I did, ready to take arms against writs of assistance." 10 Works of John Adams 247-248 (C. Adams ed. 1856). According to Adams, Otis's speech was "the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born." Id., at 248 (quoted in Boyd v. United States, 116 U.S. 616, 625 (1886)).

Riley v. California, 134 S.Ct. 2473, 2494 (2014); see also United States v. Galpin, 720 F.3d 436, 445 (2d Cir. 2013) (the Fourth Amendment was framed in opposition to the "indiscriminate searches and seizures conducted by the British under the authority of general warrants.") (quoting Payton v. New York, 445 U.S. 573, 583 (1980)) (internal quotes omitted).

The Supreme Court has long been concerned with general warrants and the unbridled authority they give to law enforcement agents to engage in boundless rummaging. As the Court noted in 1981,

> [t]he general warrant specified only an offense . . . and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched. Similarly, the writs of assistance used in the Colonies noted only the object of the search . . . and thus left . . . officials completely free to search any place where they believed such goods might be. The central objectionable feature of both warrants was that they provided no judicial check on the determination of the executing

> officials that the evidence available justified an intrusion into any particular home.

Steagald v. United States, 451 U.S. 204, 220 (1981).

This Court expressed the same concern, noting that

> General warrants were ones "not grounded upon a sworn oath of a specific infraction by a particular individual, and thus not limited in scope and application." Maryland v. King, ___ U.S. ___, 133 S.Ct. 1958, 1980 (2013). The British Crown had long used these questionable instruments to enter a political opponent's home and seize all his books and papers, hoping to find among them evidence of criminal activity. See Stanford v. Texas, 379 U.S. 476, 482–83 (1965). The Framers abhorred this practice, believing that "papers are often the dearest property a man can have" and that permitting the Government to "sweep away all papers whatsoever," without any legal justification, "would destroy all the comforts of society." Entick v. Carrington, 95 Eng. Rep. 807, 817–18 (C.P. 1765).

United States v. Ganias, 755 F.3d 125, 134 (2d Cir. 2014).

No warrant, therefore, may issue "unless probable cause is properly established and the scope of the authorized search is set out with particularity." Kentucky v. King, 563 U.S. 452, 459 (2011). This particularity requirement "makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another." Marron v. United States, 275 U.S. 192, 196 (1927). The warrant must describe with particularity the place to be searched and items to be seized, and the search and seizure must correspond to those specific parameters, United States v. Voustianiouk, 685 F.3d 206, 211 (2d

Cir. 2012), leaving "nothing . . . to the discretion of the officer executing the warrant." Marron, 275 U.S. at 196.

This Court has explicitly held that a warrant to search the contents of laptops and storage devices, without a description of the exact items in which the police were to search, violates the particularity requirement of the Fourth Amendment. United States v. Rosa, 626 F.3d 56, 62 (2d Cir. 2010). Indeed, the particularity requirement is "much more important" when a warrant permits a search of a digital device, id. at 62 (quoting United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009)), and any government position "that the entire contents of . . . computers and related storage media could be searched under the terms of [a] warrant leads to the evisceration of the Fourth Amendment's requirement of an *ex ante* probable cause determination." Id. at 62 n. 2.

C. Updating the Fourth Amendment: new technology, new interpretations, keeping faith with privacy

Fourth Amendment jurisprudence bends toward protecting individuals' privacy rights by remaining faithful to the Framers' concerns while responding to new technologies — the *application* of the Fourth Amendment has changed, but its concern with privacy, expressed in the requirement of a limiting statement of particularity, has not and in the digital realm, should not.

Fourth Amendment jurisprudence originally entailed an exclusively property law-oriented analysis based on concepts of trespass. See Olmstead v.

United States, 277 U.S. 438 (1928). At a time when individuals' papers and effects were stored almost solely on their private property, the trespass approach made sense because it ensured citizens' privacy in light of contemporary patterns of life and communication. New technologies inevitably put strains on that approach, and courts, time after time, have successfully adapted originalist Fourth Amendment jurisprudence to respond to those new technologies.

The Pony Express, for example, began its service in 1860 and raised the issue of mail privacy. This new communicative technology led to the innovative holding in Ex Parte Jackson, which held that Fourth Amendment protections extended to individuals' missives, closed against inspection and sent through the post. 96 U.S. 727, 733 (1877); see also United States v. Jacobsen, 466 U.S. 109, 113-14 (1984).

In Olmstead, the Supreme Court confronted the disruptive technology of telephone service, holding that attaching a wire to a telephone line leaving someone's private residence was not a Fourth Amendment violation because the Amendment could not be "extended and expanded to include telephone wires, reaching to the whole world." 277 U.S. at 465. Soon, however, the Court recognized that new communicative technologies required it to untether its jurisprudence from the once-universally applicable trespass approach.

The Court therefore recognized that just as individuals' communications and private information had begun to extend beyond the confines of their private property, these individuals' Fourth Amendment protections had to follow. Katz v. United States reconfigured Fourth Amendment jurisprudence to focus not on trespass theory, but on a person's expectation of privacy. 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring). While Katz entailed a new application of the Fourth Amendment, it fell directly in line with the Framers' desire to protect people's privacy, wherever that privacy was expressed.

Courts since Katz have been remarkably effective in confronting originalist Fourth Amendment principles in light of fast-changing technology. In Kyllo v. United States, the Supreme Court considered the constitutionality of an officer's use of an infrared heat detection device to virtually peer into someone's home — even though the device detected only heat *emanating from* the home. 533 U.S. 27 (2001). The Court rejected a formalistic reading of jurisprudence in favor of protecting individuals against the intrusiveness of new surveillance technology:

> We rejected such a mechanical interpretation of the Fourth Amendment in Katz, where the eavesdropping device picked up only sound waves that reached the exterior of the phone booth. Reversing that approach would leave the homeowner at the mercy of advancing technology — including imaging technology that could discern all human activity in the home. While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.

Id. at 35-36.

In United States v. Jones, the Court recognized that a formalistic interpretation of the plain view doctrine had to give way to a new jurisprudence in light of GPS tracking. In that case, the Court held that tracking a driver for 28 days constituted a search, even though the driver was tracked only while on public streets. 132 S.Ct. 945 (2012).

And in Riley v. California, the Court held that during a search incident to arrest, officers are permitted to search the contents of a cell phone only if they obtain a warrant, 134 S.Ct. 2473, because cell phones today "place vast quantities of personal information literally in the hands of individuals." Id. at 2485. Thus, Fourth Amendment jurisprudence in the "context of physical objects" has little "force with respect to digital content on cell phones." Id. at 2484. The Court clarified that its holding applies to computers as well as cell phones: "The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers . . . . One of the most notable distinguishing features of modern cell phones is their immense storage capacity." Id. at 2489.

This Court recognized the need for a new application of the Fourth Amendment in Ganias, remarking that "[a]pplying 18th Century notions about searches and seizures to modern technology . . . is easier said than done, as we are asked to measure Government actions taken in the 'computer age' against

Fourth Amendment frameworks crafted long before this technology existed." 755 F.3d at 133 (footnote omitted). Thus, this Court's "challenge is to adapt traditional Fourth Amendment concepts to the Government's modern, more sophisticated investigative tools." Id. at 134.

Fourth Amendment jurisprudence, indeed, must meet privacy demands when the Government asks a magistrate judge for a warrant to search a digital device or, essentially, the entirety of a target's life. See Riley, 134 S.Ct. at 2490 (computers become "a digital record of nearly every aspect of [users'] lives — from the mundane to the intimate.").

D. The need for particularity and why it wasn't met in Ulbricht's case

"[T]he computer hard drive [is] akin to a residence in terms of the scope and quantity of private information it may contain." Galpin, 720 F.3d at 446. Where, therefore, "the property to be searched is a computer hard drive, the particularity requirement assumes even greater importance." Id. The use of traditional, obsolete particularity statements in the digital context is fraught:

> *The potential for privacy violations occasioned by an unbridled, exploratory search of a hard drive is enormous*. This threat is compounded by the nature of digital storage. Where a warrant authorizes the search of a residence, the physical dimensions of the evidence sought will naturally impose limitations on where an officer may pry: an officer could not properly look for a stolen flat-screen television by rummaging through the suspect's medicine cabinet, nor search for false tax documents by viewing the suspect's home video collection. Such limitations are largely absent in the digital realm, where the size or other outwardly visible characteristics of a file may disclose nothing about its

content.

Id. at 447 (emphasis added). The Tenth Circuit echoed this sentiment:

> The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important.

Otero, 563 F.3d at 1132 (cited favorably in Rosa, 626 F.3d at 61-62).

Accordingly, this Court mandates "a heightened sensitivity to the particularity requirement in the context of digital searches" and, just as in Kyllo and Jones, has expressed doubt as to the availability of the plain view exception in the case of digital searches. Galpin, 720 F.3d at 447, 451.

Stating particularity, therefore, cannot be business as usual when it comes to issuing warrants to search digital data. This Court knows that, but the magistrate and the District Court in the instant case did not.

The District Court rejected Ulbricht's particularity claim, countenancing the government's seizure of "the entirety of [Ulbricht's] laptop and data on the hard drive of that laptop . . . , along with the entirety of the accounts." (District Court Docket Entry No. 89, at 29).

The District Court gave Ulbricht's argument short shrift. But the warrants permitted a search for virtually anything and everything, including "any communications or writings by Ulbricht, which may reflect . . .

political/economic views associated with 'Dread Pirate Roberts' (*e.g.*, views associated with the Mises Institute"[2]; "any evidence concerning Ulbricht's travel or patterns of movement"; "any other evidence" implicating Ulbricht in the subject crimes; and "[a]ny evidence concerning [Ulbricht] relevant to the investigation of the SUBJECT OFFENSES, including but not limited to . . . any communications or writings by ULBRICHT; . . . any evidence concerning ULBRICHT'S travel or patterns of movement." (Blue Br. 99).

Since "any" means "all," United States v. Rodriguez, 775 F.3d 533, 537 (2d Cir. 2014) (quoting United States v. Maxwell, 285 F.3d 336, 341 (4th Cir. 2002)), these warrants permitted officers literally to search and seize *all* of Ulbricht's communications, writings, evidence of his movements and travels, and *all* evidence that officers executing the search, in their discretion, deemed relevant. The Tenth Circuit has, appropriately, not countenanced warrants that permit officers to search for "anything," because such warrants authorize precisely the kind of "wide-ranging exploratory searches that the Framers intended to prohibit." United States v. Riccardi, 405 F.3d 852, 862 (10th Cir. 2005) (quoting Maryland v. Garrison, 480 U.S. 79, 84 (1987)).

[2] The Mises Institute refers to itself as the center of the "Austrian Economics Movement," https://mises.org/about-mises, and is a libertarian organization headquartered in Alabama. It was started with money raised by Senator Ron Paul. Sam Tanenhaus & Jim Rutenberg, *Rand Paul's Mixed Inheritance*, NEW YORK TIMES, Jan. 25, 2014.

The District Court was profoundly mistaken in concluding that these warrants provided sufficient particularity to guide the officers who were tasked with executing them. It heralded its blithe dismissal of Ulbricht's claim by proclaiming that because the warrant "identified the laptop and the accounts by name," *everything* in the computer and accounts could be seized. (District Court Docket Entry No. 89, at 29). This is not the stuff of particularity statements, but is that of warrants that would authorize what John Adams, James Otis, and certainly the Riley Court would refer to as "rummag[ing] through homes in an unrestrained search." Riley, 134 S.Ct. at 2494.

E. What must be done in general

As this Court has made clear, formalistic commitment to outdated forms of particularity statements is not always appropriate to digital search warrants. More is needed to adapt Fourth Amendment jurisprudence to modern technology.

The starting point for this inquiry must be an acknowledgement that warranted digital searches present officers with an unprecedented amount of digital "papers[ ] and effects," as the Framers would have put it. U.S. CONST. amend. IV. The vast majority of these papers and effects will not constitute evidence of criminality, and most will pertain to private issues such as medical care, romantic relationships, political views, and so forth. The particularity

requirement cannot be read to permit a magistrate to authorize the search and seizure of *all* of these papers and effects.

To be sure, courts have, on occasion, permitted the bulk seizure of papers and effects that include both materials that are indicative of crime and those that are not. They permit such searches, however, only where there is probable cause to believe that criminal activity permeates a business subject to a search warrant, United States Postal Service v. C.E.C. Servs., 869 F.2d 184, 187 (2d Cir. 1989), and where the permission is based on the impossibility of making a particularity statement that adequately separates potentially criminal evidence from benign materials. United States v. Falkowitz, 214 F.Supp.2d 365, 388 (S.D.N.Y. 2002). Fortunately, in the digital context courts have a number of tools at their disposal to ensure that officers executing warrants have a clear mandate to perform only a limited, particularized search.

Magistrates have increasingly included pre-search instructions in digital device warrants. CDT, 621 F.3d at 1168; United States v. Bonner, 2013 WL 3829404, at *19 (S.D. Cal.); In the Matter of the Search of: 3817 W. West End, First Floor Chicago, Illinois 60621, 321 F.Supp.2d 953, 957 (N.D.Ill. 2004); In re Appeal of Application for Search Warrant, 71 A.3d 1158 (Vt. 2012); Athul K. Acharya, *Semantic Searches*, 63 DUKE L.J. 393, 409 (2013). Other courts favor the traditional post-search reasonableness analysis. United States v. Burgess, 576 F.3d 1078, 1094 (10th Cir. 2009); United States v. Grimmett, 439 F.3d

1263, 1270 (10th Cir. 2006); State v. Bizewski, 2013 WL 1849282, at *13 (Conn. Super. Ct.). We argue that pre-search instructions, judiciously applied, play a vital role in both establishing a particularity statement in a warrant and enabling a meaningful post-search reasonableness inquiry.

As to pre-search instructions, former Ninth Circuit Chief Judge Alex Kozinski's concurring opinion in CDT is instructive. In that opinion, Chief Judge Kozinski advocated for magistrates' use of five pre-search instructions. In CDT, the Ninth Circuit considered the execution of a warrant to search the digital records of Comprehensive Drug Testing, a facility that administered tests on hundreds of major league baseball players for steroid use. 621 F.3d at 1166. Although the warrant was based on probable cause to believe that only ten players had broken the law, "the government seized and promptly reviewed the drug testing records for hundreds of players in Major League Baseball (and a great many other people)." Id.

To justify its broad seizure, the government noted in its search warrant application the "generic hazards of retrieving data that are stored electronically." CDT, 621 F.3d at 1168. The magistrate judge therefore permitted the government to seize virtually all computer equipment found along with any data storage devices and related materials. Id. The magistrate did, however, require that the government employ a taint team, or a third party — not the person or entity in possession of the seized evidence and not the

agents who performed the search or members of the investigatory or prosecution team — to separate innocuous seized data from incriminating evidence, pursuant to United States v. Tamura, 694 F.2d 591 (9th Cir. 1982). CDT, 621 F.3d at 1168; see also Preventive Medicine Associates, Inc. v. Commonwealth, 465 Mass. 810, 829 (2013).

CDT is different than Ulbricht's case in one regard: in CDT, the Government admitted that its agents' intent was to take all of the digital evidence "and later on briefly peruse it to see if there was anything above and beyond that which was authorized for seizure in the initial warrant," CDT, 621 F.3d at 1171, whereas in Ulbricht's case the officers could not go beyond the warrants' particularity limits *because there were no limits*.

Judge Kozinski's response was to offer five pre-search instructions that magistrates could include in warrants to ensure particularity:

> 1. Magistrate judges should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.
>
> 2. Segregation and redaction of electronic data must be done either by specialized personnel or an independent third party. If the segregation is to be done by government computer personnel, the government 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.

Id. at 1180 (Kozinski, CJ., concurring) (citations omitted).

The Vermont Supreme Court has discussed why appropriate use of these pre-search instructions is vital, observing:

> In the digital universe, particular information is not accessed through corridors and drawers, but through commands and queries. As a result, in many cases, the only feasible way to specify a particular 'region' of the computer will be by specifying how to search. We view such ex ante specification as an acceptable way to determine particularity.

In re Appeal of Application for Search Warrant, 71 A.3d at 1171.

In the digital context, particularity may require use of some or all of these pre-search instructions. These instructions should be used to ensure that warrants do what they have always done: prohibit officers from searching locations they have no probable cause to search. Such instructions ensure particularity by identifying whether the hardware itself is evidence of a crime, i.e. contains contraband or is contraband, or is an instrumentality of a crime, or if the hardware simply stores evidence of a crime. See Fed. R. Crim. P. 41(c); see also Office of Legal Educ. Exec. Office for United States Attorneys, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal*

Investigations, Dep't of Justice: Computer Crime and Intellectual Property Section, Criminal Division, 63 (2009), http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf. The warrant should permit the search and seizure of relevant computer files rather than the digital media itself. It should also identify records that relate to the particular crime for which officers have probable cause to search, including specific categories of or types of records to be found. This type of information can be discerned by, for example, the identity of the target of the search, the time frame of the crime being investigated, or the actual crime itself, like child pornography. Id. at 72-73.

The particularity requirements for a warrant to search for digital evidence should be detailed enough to clearly and unambiguously inform law enforcement as to what is included and what is not included within the scope of the approved search. To accomplish that objective, the articulation of the specific target of the search must utilize the narrowest particulars necessary to discriminate between what is and is not to be searched.

Take, for example, a search of a personal laptop computer to obtain evidence of a physician's alleged illegal distribution of pain medications. The warrant first must specifically identify the physical address where the computer is to be found and the location on the premises where it is located. The warrant must also specify the type of computer to be searched (in this case a specific

make of laptop), and then specify the type and content of digital files to be searched. Such file types and content would be limited in this example to text documents in which search queries reveal the presence of the doctor's DEA number, names and addresses of patients referenced in the allegedly illegal prescriptions, and emails to and from those patients. Without more supporting investigative information, the image files on the computer, other emails, and personal documents not specific to the doctor's prescription authority would be excluded from the warrant to search. Such particularities carve out the scope of the warranted search from the general population of files stored on the laptop.

Search protocols should be outlined for how the government plans to conduct onsite and offsite searches of digital devices, and can be suggested by government agents when they apply for warrants. Agents should explain how these protocols will keep their search within the bounds of the warrant. Such protocols may include the use of a taint team, restrictions on information sharing between the taint team and law enforcement investigators and prosecutors, obtaining a warrant when evidence of a separate crime is legitimately within plain view, the use of search terms, and the use of forensic software.

Pre-search instructions are vital to meaningful post-search reasonableness inquiries that every magistrate must perform. After all, with no

pre-search instructions in the digital context, officers will be authorized by the warrant to perform a virtual basement-to-attic sweep of every nook and cranny of a computer. If their search is not bounded by pre-search instructions, then nothing is unreasonable. This certainly cannot be the judiciary's (non-)response to new technology.

The Tenth Circuit recognized the inextricable connection between pre-search instructions and post-search reasonableness, writing that the provision of and adherence to the former will contribute greatly to a reasonableness analysis favorable to the government:

> This isn't to say the Fourth Amendment has nothing to say on *how* a computer search should proceed. Even putting aside for the moment the question what limitations the Fourth Amendment's particularity requirement should or should not impose on the government *ex ante*, the Amendment's protection against "unreasonable" searches surely allows courts to assess the propriety of the government's search methods (the *how*) *ex post* in light of the specific circumstances of each case. See, e.g., United States v. Ramirez, 523 U.S. 65, 71 (1998) ("The general touchstone of reasonableness . . . governs the method of execution of the warrant."); United States v. Angelos, 433 F.3d 738, 746 (10th Cir. 2006). So even if courts do not specify particular search protocols up front in the warrant application process, they retain the flexibility to assess the reasonableness of the search protocols the government actually employed in its search after the fact, when the case comes to court, and in light of the totality of the circumstances. Unlike an *ex ante* warrant application process in which the government usually appears alone before generalist judges who are not steeped in the art of computer forensics, this *ex post* review comes with the benefit, too, of the adversarial process where evidence and experts from both sides can be entertained and examined. See Burgess, 576 F.3d at 1094; United States v. Carey, 172 F.3d 1268, 1275-76

(10th Cir. 1999); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 574–75 (2005).

United States v. Christie, 717 F.3d 1156, 1166-67 (10th Cir. 2013).

To be sure, case-specific realities will drive which pre-search instructions a magistrate must include to ensure both particularity and the magistrate's ability to perform a meaningful post-search reasonableness analysis. Although they were originally fashioned as mandates, United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1006-07 (9th Cir. 2009), Chief Judge Kozinski's pre-search instructions became admonitory guidelines that magistrates should consider and impose as necessary. CDT, 621 F.3d at 1180. In addition to magistrates' role in authorizing appropriately limited searches by use of pre-search instructions, the Government should proactively self-impose them in warrant applications wherever possible.

In addition to imposing some or all of Chief Judge Kozinski's five pre-search instructions and performing robust traditional post-search reasonableness inquiries, magistrates might consider a second limitation. They could require officers to foreswear reliance on the plain view doctrine. This is important because, surprising at it may seem, the Government's admission in CDT that it fully intended to seize evidence beyond the scope of its warrant is grounded in law.

In Coolidge v. New Hampshire, the Supreme Court first explicitly

established that to rely on the plain view doctrine to seize evidence that was beyond the scope of a warrant, agents must have arrived at the evidence inadvertently. 403 U.S. 443, 469-70 (1971). In turn, where "discovery is anticipated," agents could not rely on plain view. Id. at 470.

Nearly 20 years later, however, in Horton v. California, the Court rejected the inadvertence requirement, 496 U.S. 128, 137 (1990), mandating only that agents come to evidence in plain view lawfully — that is, within the scope of the warrant — and that the incriminating character of the evidence be "immediately apparent." Horton, 496 U.S. at 136. This means that during a warranted search for evidence of credit card fraud, if agents come across a folder labeled "kiddiepornpics," agents may nevertheless perform a detailed search of the contents of that folder, even if they intend to find evidence of child pornography and not credit card fraud. See United States v. Kim, 677 F.Supp.2d. 930, 945, 949-50 (S.D. Tex. 2009). This is so because of the general non-discernibility of digital evidence; a file labeled "kiddiepornpics" could *technically* contain evidence of credit card fraud. It does not matter that most people would think it unreasonable to believe that evidence of credit card fraud would be hidden in such a folder. In the digital context, the Government would argue, this means that once a warrant to search digital devices issues, agents may search the entirety of the devices, even if they are attempting and expecting to find evidence of *any* crime (or even any unpopular, but legal,

conduct), whether or not it is set forth in the warrant. This is the very definition of unbounded rummaging that the Fourth Amendment's particularity requirement abhors.

The way to avoid this unbounded rummaging is two-fold. First, magistrates could require agents to foreswear reliance on plain view, meaning that if they have a warrant to search for evidence of crime A, they may perform a search only for evidence of crime A; if they believe they may capture evidence of crime B, they may not use the technical authorization of the warrant and Horton to go beyond the search for evidence of crime A; to do so would constitute an unreasonable, extrajudicial fishing expedition.

Second, foreswearing reliance on plain view does not mean that agents will be unreasonably hobbled in their good-faith efforts to uncover evidence of crime A. Agents may certainly search for evidence of crime A in a reasonable manner, as bounded by the magistrate's pre-search instructions, and need not fear losing evidence of crime B should they inadvertently come across it. If they do unexpectedly uncover evidence of crime B, however, they should immediately stop the search, freeze the scene, and seek a warrant to search for evidence of crime B (their warrant to search for evidence of crime A would, of course, still be in effect).

Courts have suggested that this two-step process is reasonable and may be necessary to ensure particularity in digital warrants and searches. The

Massachusetts Supreme Judicial Court expressed its concern that

> a cursory review of every e-mail undermines the particularity requirement of the Fourth Amendment and art. 14 [of the U.S. Constitution], particularly where . . . the cursory review is joined with the plain view doctrine to enable the Commonwealth to use against the defendants inculpatory evidence with respect to the pending indictments that it finds in the emails, even though such evidence may not actually fit within the scope of the search warrants obtained.

Preventive Medicine Associates, Inc., 465 Mass. at 831-32. Similarly, Fourth Amendment scholar Orin Kerr has argued that "computer technologies may allow warrants that are particular on their face to become general warrants in practice." *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 565 (2005). And Paul Ohm has observed that "[c]omputer search warrants are the closest things to general warrants we have confronted in the history of the Republic." *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. IN BRIEF 1, 11 (2011).

F. What should have been done in Ulbricht's case

Ulbricht does not, of course, bear any burden to show *how* the magistrate might have drafted a warrant that included an adequate particularity statement; he only needs to show *that* the warrant lacked such a statement. Nevertheless, how the magistrate might have drafted an adequate particularity statement is not difficult to show, and doing so illustrates why, in the instant case, the warrants provided no particularity. There are at least five particularized

alternatives to the District Court's warrant language that demonstrate practicable approaches to ensuring effective law enforcement and satisfaction of the constitutional necessity of particularity.

First, the District Court indicated that Ulbricht's computer was "likely to contain evidence concerning ULBRICHT relevant to the investigation of the SUBJECT OFFENSES, including evidence relevant to corroborating the identification of ULBRICHT as the Silk Road user 'Dread Pirate Roberts.'" (Blue Br. 99). Presumably, prior to seeking the warrants at issue, law enforcement agents had amassed evidence that a certain party was engaged in online criminal conduct as the Dread Pirate Roberts. Agents would, therefore, be aware of the particular screen name(s) or online handle(s) that this person used when operating as the Dread Pirate Roberts. He or she could have gone by "Dread Pirate Roberts," "DPR," "Dread," and so forth. Any online handle used by this person would be inevitably stored in that person's computer, and subject to a word or term search. The magistrate, therefore, could have authorized a very broad, but particularized search for documents, texts, Internet activity, and anything else containing "Dread Pirate Roberts," "DPR," "Dread," "Pirate," "Roberts," and any other relevant word or combination of words.

Second, the magistrate authorized a search for "any communications or writings by Ulbricht, which may reflect linguistic patterns or idiosyncrasies

associated with 'Dread Pirate Roberts'[] or political/economic views associated with 'Dread Pirate Roberts.'" (Blue Br. 99). Again, we presume that agents were familiar with these linguistic patterns and idiosyncrasies prior to seeking the search warrants, for if they had not been, then this warrant truly would authorize a fishing expedition without any basis in probable cause. Since agents were familiar with these patterns and idiosyncrasies, they would have been able to identify the unique words, phrases, spellings, and so forth associated with Dread Pirate Roberts. These words, phrases, and spellings are eminently susceptible to key word and phrase searching on a computer. The magistrate could have permitted a search only for these idiosyncrasies.

Third, the magistrate authorized a search for "any evidence concerning Ulbricht's travel or patterns of movement, to allow comparison with patterns of online activity of 'Dread Pirate Roberts' and any information known about his location at particular times." (Blue Br. 99). Here again, agents must have been aware of the dates that the online Dread Pirate Roberts was travelling or located in certain places that they wanted to compare against evidence found on Ulbricht's computer. The magistrate could have authorized a search only for files and computer activity associated with these dates and locations. This would have been easy to do: date-limited searches of hard drives is a routine process, and if agents were aware of the online Dread Pirate Roberts' location in the physical world, it would be by tracing IP addresses, also readily

searchable on Ulbricht's computer.

Fourth, the magistrate authorized a search for "any other evidence implicating ULBRICHT in the SUBJECT OFFENSES." (Blue Br. 99). This catch-all global authorization is not tied to any evidence agents might have presented to the magistrate, and thus there is absolutely no probable cause supporting it. This authorization should simply not have been included.

Fifth, the magistrate did not, but could have required the use of a neutral taint team to separate the innocuous content of Ulbricht's laptop and social media accounts from any incriminating matter that might have been discovered therein.

CONCLUSION

Digital devices store unprecedented amounts of data, including text documents, financial records, images, videos, e-books, web search histories, and other data that touch on virtually every aspect of a user's life. Without some cursory inspection, each file can appear to be indistinguishable from any other file. Simply opening the cover of a laptop will not reveal a box of family photos next to a medical bill next to an illegal narcotics ledger. The massive amount of sometimes-indistinguishable data presents new Fourth Amendment challenges to magistrates who endeavor to provide constitutionally-required particularity statements in the warrants they issue.

Just as courts have responded to disruptive technology in the past, courts are now generating new types of particularity statements that ensure individuals' privacy and do not hobble law enforcement efforts. Pre-search instructions and robust post-search reasonableness inquiries connected to those instructions are the loci of courts' response.

This Court should adopt that framework in reviewing the adequacy of digital search warrants by issuing a detailed opinion discussing its view of pre-search instructions and requiring lower courts to engage in robust post-search reasonableness inquiries. This Court should also acknowledge the inextricable link between imposition of pre-search instructions and the ability to perform meaningful post-search reasonableness inquiries.

Ulbricht's specific case is much simpler, because the warrants to search his digital device and accounts lacked *any* particularity and the District Court judge engaged only in a blithe dismissal of his claims, not a genuine post-search reasonableness analysis. This Court should, therefore, reverse the District Court's denial of his motion to suppress, vacate his conviction, and remand to District Court for a new trial consistent with this Court's opinion.

Dated: January 18, 2016
Grand Forks, North Dakota

Respectfully submitted,

Steven R. Morrison

Steven R. Morrison
University of North Dakota
School of Law
1526 Robertson Court
Grand Forks, ND 58201
(617) 749-7817

Joel B. Rudin
Law Offices of Joel B. Rudin, P.C.
600 Fifth Avenue, 10th Floor
New York, NY 10020
(212) 752-7600

Attorneys for Amicus Curiae National Association of Criminal Defense Lawyers

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(a)(7)(C), I hereby certify that this brief complies with the type-volume limitations of Fed. R. App. P. 29(d) and 32(a) because it was produced using Garamond typeface in 14-point font and contains 6,895 words, excluding the parts of the brief exempted by Rule 32(a)(7)(B)(iii), according to the word processing system I utilized.

Dated: January 18, 2016
Grand Forks, North Dakota

Steven R. Morrison
Steven R. Morrison

CERTIFICATE OF SERVICE

I hereby certify that on this date a copy of the foregoing was filed electronically with the Court's CM/ECF system. Notice of this filing will be sent by email to all parties by operation of the Court's electronic filing system. Parties may access this filing through the Court's CM/ECF system.

Dated: January 18, 2016
Grand Forks, North Dakota

Steven R. Morrison
Steven R. Morrison