FOURTH AMENDMENT FUTURE: REMOTE COMPUTER SEARCHES AND THE USE OF VIRTUAL FORCE

*Susan W. Brenner**

INTRODUCTION 1229
I. TROJAN HORSE WARRANTS? 1232
A. Europe 1232
B. United States 1237
C. Search 1238
D. Seizure 1244
E. Trojan Horse Warrants 1246
F. Exceptions 1251
II. VIRTUAL FORCE? 1253
CONCLUSION 1259

INTRODUCTION

For roughly the first 130 years of its existence, the Fourth Amendment, unlike other components of the Bill of Rights, was not a problematic constitutional provision.[1] It started to become problematic in the 1920s, as new technologies—such as automobiles and telephones—became more widely used.[2]

As the twentieth century progressed, the Fourth Amendment's applicability (or inapplicability) to the technologies that emerged and matured after 1900, but before 2000, was more

* NCR Distinguished Professor of Law and Technology, University of Dayton School of Law, Dayton, OH. Email: susanwbrenner@yahoo.com.

[1] The Bill of Rights became effective on December 15, 1791. *See, e.g.*, LEONARD W. LEVY, ORIGINS OF THE BILL OF RIGHTS 42-43 (2001).

[2] *See, e.g.*, Thomas K. Clancy, Symposium, *The Effect of Technology on Fourth Amendment Analysis and Individual Rights,* 72 MISS. L.J. 1, 2-3 (2002) (noting Supreme Court cases dealing with twentieth-century technologies); *see also* Russell L. Weaver, *The Fourth Amendment, Privacy and Advancing Technology,* 80 MISS. L.J. 1131, 1138-40 (2011).

or less settled.[3] Ambiguities and uncertainties remain in certain areas, but the Fourth Amendment jurisprudence of the pre-twenty-first century technologies is relatively stable.[4]

That is not true of the digital technologies that emerged in the last decades of the twentieth century and have been evolving in sophistication and complexity ever since. Unlike their essentially stable predecessors, which tended to have specific uses, these technologies infiltrate many, if not most, areas of human endeavor.[5] We use them to communicate, to create, to navigate, to heal, to manufacture, to educate, to forecast, to research, to surveil, to attack, etc.

Perhaps the feature that most distinguishes these technologies from their more mundane predecessors is that they facilitate human activity in what is—or in what we experience as—a non-physical context. Computers and other electronic devices let us "go into" cyberspace, which, of course, is not a "space" at all, but is a conduit we can use to generate effects—consequences—that are felt in the physical world.[6]

The pervasiveness and consequential nature of digital technologies make them an increasingly important aspect of our lives, which means, among other things, that they are used by the lawless as well as the law-abiding. In the 1920s, the Supreme Court was called upon to determine the Fourth Amendment's applicability to two still novel technologies—automobiles and telephones—because criminals quickly grasped how they could be exploited to facilitate the commission of unlawful acts.[7]

And law enforcement officers soon grasped how they could exploit these new technologies to facilitate their pursuit of those

---

[3] *See, e.g.*, Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution,* 102 MICH. L. REV. 801, 862-64 (2004) (noting that the use of "stable" technologies facilitates the articulation of stable rules derived from the Fourth Amendment).

[4] *See, e.g.*, *id*. at 860-64.

[5] *See generally* SUSAN W. BRENNER, LAW IN AN ERA OF "SMART" TECHNOLOGY (2007); *see also* Kerr, *supra* note 3, at 864-65.

[6] *See, e.g.*, Susan W. Brenner, *The Privacy Privilege: Law Enforcement, Technology, and the Constitution*, 7 J. TECH. L. & POL'Y 123, 144-45 (2002).

[7] *See id.* at 150-53; *see also* SUSAN W. BRENNER, CYBERCRIME: CRIMINAL THREATS FROM CYBERSPACE 156 (Frankie Y. Bailery & Steven Chermak eds., 2010).

who committed unlawful acts.[8] Law enforcement's use of automobiles raised few, if any, Fourth Amendment issues, but its use of telephone surveillance produced the first case in which the Supreme Court was required to consider the implications of technology that transcends the limitations of physical reality.[9]

As many have noted, the Supreme Court misapprehended the implications of that technology, issuing a decision that was predicated on the spatial notion of privacy that had prevailed and sufficed, until that point in our history.[10] It was not until 1967 that the Court shifted away from that approach to one that is more conceptual but still retains a concern with spatial privacy.[11]

Courts now find themselves grappling with technologies that far surpass twentieth-century telephones in complexity and application. As one author noted, judges are attempting to determine the Fourth Amendment's applicability to "intrusive scanning machines, . . . handheld devices the police can use to measure the presence of alcohol on one's breath and guns and drugs on the person's body; facial recognition systems . . . and very sophisticated systems to search e-mail and computer files."[12] Of course, these are only a few of the technologies already in use that have the capacity to be exploited by law enforcement and that therefore give rise to difficult Fourth Amendment issues.[13]

These issues arise because, as our experience with automobiles and telephones illustrates, law enforcement is quick to grasp, and exploit, the enhanced capabilities new technologies provide. My goal in this Article is to project how law enforcement can and, I suspect, will, utilize two as yet unexploited aspects of digital technology: (1) the use of Trojan Horse software to conduct surreptitious, remote searches of computers[14] and (2) the use of

---

[8] *See, e.g.*, BRENNER, CYBERCRIME, *supra* note 7, at 158.

[9] *See, e.g.*, Brenner, *Privacy Privilege*, *supra* note 6, at 144-45; *see also* Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1, 20-25 (2005).

[10] *See, e.g.*, Brenner, *Ubiquitous Technology*, *supra* note 9, at 4-25.

[11] *See id.* at 25-28.

[12] Clancy, *supra* note 2, at 3.

[13] *Id.* at 4.

[14] A Trojan horse program "is a malicious code concealed within an apparently harmless [computer] program that hides its true function." U.S. DEP'T OF JUSTICE, NAT'L INST. OF JUSTICE, INVESTIGATIONS INVOLVING THE INTERNET AND COMPUTER

computer software and/or signals as "virtual force" to shut down criminal websites or otherwise impede unlawful online activity. The first section below examines remote computer searches; the next section examines virtual force.

I. TROJAN HORSE WARRANTS?

In examining the likelihood that U.S. law enforcement will eventually use Trojan Horse programs to conduct remote searches of computers, I need to address two issues. One issue essentially involves precedent—in the subsection immediately below, I review efforts to authorize the use of such searches in Europe. In the next subsection, I analyze the Fourth Amendment issues that would have to be addressed before U.S. law enforcement agencies could lawfully utilize such searches.

A. Europe

In a press release issued at the end of 2008, the European Union (EU) announced a new five-year plan to target cybercrime. [15] Among other things, the plan called for law

---

NETWORKS 55 (2007), *available at* http://www.ncjrs.gov/pdffiles1/nij/210798.pdf. Trojan Horse programs are routinely used by cybercriminals to steal information from unwary computer users or to take control of their computers. *See id.* at 1. As Timothy C. MacDonnell notes, they could also be used by law enforcement:

> In the context of the home, the government could send an email to a suspect that contains a "Trojan horse" program. Once the email was opened the program could be downloaded to the suspect's computer without his knowledge. The program would search the target computer for the hash value of known contraband files. If the program encountered a contraband file, it would alert law enforcement.

Timothy C. MacDonnell, *Orwellian Ramifications: The Contraband Exception to the Fourth Amendment*, 41 U. MEM. L. REV. 299, 346-47 (2010) (footnotes omitted); *see id.* at 347 n.335 (noting that Trojan Horse programs let the operator of the software retrieve user names and passwords stored on the target computer and "find, view, copy and delete files," among other things).

[15] *See* Press Release, Europa, Fight against Cyber Crime: Cyber Patrols and Internet Investigation Teams to Reinforce the EU Strategy (Nov. 27, 2008), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827 ("Cyber crime is a growing threat to our societies today. EU member states suffer daily thousands of attacks against their information systems. . . . The European Commission has cooperated closely with the French Presidency and the Member States in the elaboration of a series of practical measures to fight cyber crime. The new strategy

enforcement officers in EU member states to conduct "remote searches" of computers.[16]

A few months earlier:

> [T]he EU Council Presidency circulated a Note on a: "*Comprehensive plan to combat cyber crime*" to COREPER - the Council committee of Brussels-based high-level representatives of each Member State.[17]
>
> Under the sub-heading "The emergence of new issues" it said that there were some: "projects already in existence" which require "common approaches" including:
>
> "the area of remote computer searches, which are a delicate issue because of their cross-border nature." (emphasis added)
>
> Reading between the lines the phrase: "projects already in existence" implies that state agencies in some Member States are already conducting cross-border remote computer searches both in their home countries and across borders in other states.[18]

---

recommends reinforcing partnership between the police and the private sector by better knowledge-sharing on investigation methods and trends in cyber crime. It also encourages both parties to respond quickly to information requests, resort to remote searches, cyber patrols for online tracking of criminals and joint investigations across borders."); *see also EU to Search out Cyber Criminals*, BBC NEWS (Dec. 1, 2008, 10:57 GMT), http://news.bbc.co.uk/2/hi/technology/7758127.stm.

[16] *See* BBC NEWS, *supra* note 15.

[17] Tony Bunyan, *EU Agrees Rules for Remote Computer Access by Police Forces—But Fails, as Usual, to Mention—the Security and Intelligence Agencies*, 19 STATEWATCH J., Aug. 2009, at 1, *available at* http://www.statewatch.org/analyses/no-83-remote-computer-access.pdf; *see also* Lesley Dingle & Bradley Miller, *A Summary of Recent Constitutional Reform in the United Kingdom*, 33 INT'L J. LEGAL INFO. 71, 94 (2005) ("'The Council [of the European Union] is the main decision-making body of the European Union . . . [its] acts . . . can take the form of regulations, directives, decisions, . . . recommendations or opinions. The Council can also adopt conclusions . . . . When the Council acts as a legislator, in principle it is the European Commission that makes proposals. These are examined within the Council, which can modify them before adopting them.' The Council is obliged to 'consult' [the European] Parliament on its acts, . . . but should disagreement arise, the Council can dispense with Parliament's opinion." (footnotes omitted)).

[18] Bunyan, *supra* note 17, at 2.

This note became the basis of a "proposal for formal Council 'Conclusions,'" which eventually called for "measures to facilitate remote computer searches, allowing investigators rapid access to data."[19] The final, adopted version called for "facilitating remote searches if provided for under national law, enabling investigation teams to have rapid access to information, with the agreement of the host country."[20]

Neither the initial press release nor the subsequent news stories explained precisely what these "remote searches" would involve. Some speculated that they might involve using remotely installed keystroke loggers, an updated version of the Federal Bureau of Investigation's "Magic Lantern" program.[21] According to one source, the FBI created Magic Lantern

> primarily to overcome the problems raised by suspects who were savvy enough to encrypt their data. It operates in the following manner. The FBI first installs Magic Lantern directly onto the suspect's computer by way of a Trojan horse virus, sent via email. Once installed, the software records every single keystroke that the suspect types. The FBI can then secretly break into the suspect's home to download the recorded data. This data is then analyzed to determine the suspect's encryption passwords. With these passwords, the FBI can then gain access to all of the suspect's encrypted data, without his knowledge.[22]

In 2006, a German attorney general sought a warrant from "the investigating judge of the federal court" that would authorize

---

[19] *Id.* (citation omitted) (internal quotation marks omitted).

[20] Council of the European Union, Draft Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime, No. 15569/08 of 11 Nov. 2008, at 5, *available at* http://register.consilium.europa.eu/pdf/en/08/st15/st15569.en08.pdf.

[21] *See, e.g.*, Wiebke Abel & Burkhard Schafer, *The German "Federal Trojan"—Challenges Between law and Technology*, TEUTAS L. & TECH. (Mar. 2, 2009, 17:48 GMT), *available at* http://www.teutas.it/societa-informazione/prova-elettronica/634-the-german-federal-trojan-challenges-.

[22] Ginger Vaudrey, *The Technology of National Security*, L. TECH., Jan. 1, 2004, *available at* 2004 WLNR 15265384 (footnotes omitted).

German police "to search a suspect's computer using an RFS [remote forensic tool]."[23] The application sought permission

> to investigate the data stored on the hard disk and the working memory of the computer. To accomplish this, a specifically designed computer program was to be planted on the suspect's computer without raising his suspicion. This program would then copy all data stored on the computer and subsequently transfer it back to the investigating authority for evaluation. In addition to files stored on the computer, access was also asked for email traffic and information about visited websites.[24]

When the judge declined to issue the warrant, the attorney general appealed to the federal court (the Bundesgerichtshof), which held that the warrant could not be issued because "no legal authorisation existed . . . under German law permitting the use of RFS tools in crime investigations by law enforcement agencies."[25] At around the same time, another German state adopted legislation that authorized the use of remote computer searches (or remote forensic tools), among other things.[26] A complaint was filed with the German Federal Constitutional Court (Bundesverfassungsgericht), challenging the constitutionality of this legislation.[27] On February 27, 2008, the Federal Constitutional Court held that it violated the German Constitution and was therefore unlawful and unenforceable.[28]

The "remote forensic tools" at issue in these cases apparently involved the use of Trojan Horse programs.[29] They seem to be at least one of the tools British police can utilize in carrying out

---

[23] Abel & Schafer, *supra* note 21; *see also German Police Seeks Legal Permission for Online House Search*, SPAMFIGHTER (Mar. 14, 2007), http://www.spamfighter.com/News-7911-German-Police-Seeks-Legal-Permission-for-Online-House-Search.htm.

[24] Abel & Schafer, *supra* note 21.

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.* (The authors note that either computer viruses or Trojan Horse programs could be used, but they tend to emphasize the use of Trojan Horse programs.).

"intrusive surveillance" of certain suspects.[30] The Regulation of Investigatory Powers Act of 2000 (RIPA) gives certain officials the authority to authorize such surveillance.[31] An official cannot authorize intrusive surveillance unless he or she determines that it is necessary (i) "in the interests of national security"; (ii) to prevent or detect "serious crime"; or (iii) "in the interests of the economic well-being of the United Kingdom."[32] Intrusive surveillance can be authorized even if it "includes conduct outside the United Kingdom."[33]

RIPA defines intrusive surveillance as surveillance that is "carried out in relation to anything taking place on any residential premises" and "involves the presence of an individual on the premises . . . or is carried out by means of a surveillance device."[34] Surveillance that is carried out "by means of a surveillance device in relation to anything taking place on" residential premises or is carried out "without that device being present on the premises . . . is not intrusive unless the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises . . . ."[35]

According to the BBC, in 2009, the British Home Office "signed up to an EU strategy that 'encourages' police . . . to remotely access personal computers."[36] The story notes that British police already had the ability to conduct such searches and that a spokesman for the Association of Chief Police Officers told a reporter that "police were already carrying out a small number of these operations" each year.[37]

---

[30] *See, e.g.*, Flora Graham, *Police 'Encouraged' to Hack More*, BBC NEWS (Jan. 5, 2009, 18:04 GMT), http://news.bbc.co.uk/2/hi/7812353.stm (discussing the use of Trojan Horse programs).

[31] *See* Regulation of Investigatory Powers Act, 2000, c. 23, § 32(1) (Eng.) ("[T]he Secretary of State and each of the senior authorising officers shall have power to grant authorisations for the carrying out of intrusive surveillance.").

[32] *Id.* at c. 23, § 32(2)-(3).

[33] *Id.* at c. 23, § 27(3).

[34] *Id.* at c. 23, § 26(3).

[35] *Id.* at c. 23, § 26(5).

[36] Graham, *supra* note 30.

[37] *Id.*

I cannot find any information as to whether other members of the EU have followed Britain's lead and incorporated remote computer searches into their criminal procedure. My suspicion, and it is just that, is that most EU countries are not using remote computer searches because the authority to conduct such searches currently does not exist under their national laws.[38] Some of them may eventually decide to follow Britain's lead and adopt legislation that authorizes remote computer searches; others may side with Germany, concluding that such searches cannot be authorized under their foundational law. This brings us to the Fourth Amendment.

B. United States

The Fourth Amendment creates a right to be free from "unreasonable searches and seizures."[39] A Fourth Amendment violation occurs when there is (i) a search and/or seizure that (ii) is conducted by law enforcement[40] and (iii) is not "reasonable."[41]

In determining whether there has been a violation of the Fourth Amendment, courts begin not with whether the law enforcement conduct at issue was "reasonable," but with whether it resulted in a "search" and/or a "seizure."[42] A "search" violates a "reasonable expectation of privacy" in a place or a thing.[43] To have such an expectation of privacy, one must subjectively believe the

---

[38] *See supra* note 20 and accompanying text.

[39] U.S. CONST. amend. IV.

[40] *See, e.g.*, United States v. Aldridge, 642 F.3d 537, 541 (7th Cir. 2011) ("The Fourth Amendment generally does not apply to searches and seizures by private parties, but it does apply if the private party is acting as a government agent.").

[41] In this Section, I am assuming the Fourth Amendment applies to law enforcement-initiated remote computer searches. Under current law, that (i) is true if the computer being searched is in the territorial United States or is owned by a U.S. citizen and (ii) is not true if the computer is outside the territorial United States and is not owned by a U.S. citizen. *See, e.g.*, United States v. Verdugo-Urquidez, 494 U.S. 259, 269-75 (1990). I, for one, suspect the second alternative is not a viable way to proceed, at least with regard to networked computer searches, because it can create tensions between nations. *See, e.g.*, Susan W. Brenner & Bert-Jaap Koops, *Approaches to Cybercrime Jurisdiction*, 4 J. HIGH. TECH. L. 1, 21-23 (2004).

[42] *See, e.g.*, Boroian v. Mueller, 616 F.3d 60, 65 (1st Cir. 2010) (explaining that the threshold question to be resolved was whether there was a search or seizure; then having found that a search occurred, the court then determined its reasonableness).

[43] *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 211 (1986).

area or object is private and society must accept that belief as objectively reasonable.[44] A "seizure" of someone's property occurs when "there is some meaningful interference with an individual's possessory interests in that property."[45] To be "reasonable," a search or seizure must be conducted pursuant to a warrant or pursuant to an applicable exception to the warrant requirement.[46]

U.S.-initiated remote searches of the type authorized by RIPA, and sanctioned by the EU Council, will therefore violate the Fourth Amendment if they are (i) conducted by law enforcement, (ii) result in a search and/or seizure within the compass of the Fourth Amendment and (iii) are not "reasonable." I will assume, for the purposes of analysis, that the hypothesized remote searches under consideration in this Article *are* conducted by law enforcement officers, which brings us to the question of whether this activity results in a "search" and/or a "seizure."

C. Search

We will begin with searches. The use of a Trojan Horse program (or similar malware) to investigate the contents of someone's computer will constitute a "search" if the person had a reasonable expectation of privacy in the contents of that computer's hard drive. Not surprisingly, there seems to be no reported decisions that are precisely on point,[47] but courts have

---

[44] *See, e.g.*, *Boroian*, 616 F.3d at 60, 65 ("whether a search or seizure had occurred" was the threshold question, to be resolved initially; having found that a search occurred, the court then determined its reasonableness); *see also* Katz v. United States, 389 U.S. 347, 351 (1967).

[45] Soldal v. Cook Cnty., 506 U.S. 56, 61 (1992) (quoting United States v. Jacobsen, 466 U.S. 109, 113 (1984)) (internal quotation marks omitted).

[46] *See, e.g.*, United States v. Butler, 405 Fed. App'x 652, 655 (3d Cir. 2010).

[47] In *United States v. Steiger*, the defendant moved to suppress evidence obtained from his computer, arguing that the search warrant for the computer was invalid "because it was based in part on information from an anonymous source who hacked into his computer." 318 F.3d 1039, 1045 (11th Cir. 2003). In communications to law enforcement, the anonymous source claimed to have used a Trojan Horse program to "enter into Steiger's computer via the Internet" and download evidence which he then sent to police. *Id.* at 1043-45. The Eleventh Circuit held that suppression was not in order because the anonymous source "acted at all material times as a private individual," and the Fourth Amendment does not apply to the conduct of private

held that individuals have a reasonable expectation of privacy in the contents of their computer hard drives, unless they have taken actions that nullify that expectation.[48]

They have analogized a computer's hard drive to a "container," and found that absent countervailing circumstances,[49] hard drives are accorded protection "similar to the protection [the Fourth Amendment] affords a person's closed containers and closed personal effects."[50] Since individuals have a presumptively reasonable expectation of privacy in closed containers,[51] it follows that they have a reasonable expectation of privacy in computer "containers," unless they have taken actions that diminish or defeat that expectation of privacy.

In analyzing the potential Fourth Amendment implications of remote computer searches, I shall assume such searches target computers located in an individual's home or office. I make that assumption because it adds a dimension to the analysis. [52]

---

citizens. *Id.* at 1045; *accord* United States v. Jarrett, 338 F.3d 339, 346-47 (4th Cir. 2003).

[48] *See, e.g.*, United States v. Leiske, No. 08-CR-453-KI, 2011 WL 3205308, at *6 (D. Or. July 27, 2011); United States v. Barth, 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998); Commonwealth v. Cormier, No. 09-1365, 2011 WL 3450643, at *3-4 (Mass. Super. Ct. June 27, 2011).

[49] For what constitutes such circumstances, see *infra* notes 58-60 and accompanying text.

[50] United States v. Barth, 26 F. Supp. 2d 929, 936-37 (W.D. Tex. 1998); *see, e.g.*, United States v. Peden, No. CR. 06-0300 WBS, 2007 WL 2318977, at *3 (E.D. Cal. Aug. 13, 2007) ("'A person has an expectation of privacy in his or her private, closed containers'" which "[u]ndoubtedly . . . extends to personal computers in one's home . . . ." (quoting United States v. Fultz, 146 F.3d 1102, 1105 (9th Cir. 1993))); People v. Carratu, 755 N.Y.S.2d 800, 807 (N.Y. Sup. Ct. 2003) ("By placing data in files on the hard drive of his computer, defendant manifested a reasonable expectation of privacy in the contents of those files."); Brackens v. State, 312 S.W.3d 831, 837 (Tex. Ct. App. 2009) ("The Fourth Amendment protection afforded to closed computer files and hard drives is similar to the protection afforded to a person's closed containers and closed personal effects."); *see also* United States v. Payton, 573 F.3d 859, 862 (9th Cir. 2009) ("Searches of computers . . . often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers."); United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007) ("[C]omputers should fall into the same category as suitcases, footlockers, or other personal items that command a high degree of privacy.").

[51] *See, e.g.*, United States v. Ross, 456 U.S. 798, 822-23 (1982); United States v. Villarreal, 963 F.2d 770, 773-74 (5th Cir. 1992).

[52] I also utilize this assumption to simplify the empirical aspects of the analysis; the conclusions derived from the home-office analysis should apply with equal force to

Traditionally, to access data on such a computer, police officers must (i) first enter the computer owner's home or office and (ii) then "enter" the computer itself. A traditional search of a computer located in a home or office involves two entries (one into the home or office, the other into the computer), each of which must be reasonable under the Fourth Amendment.

I shall also assume, again for the purposes of this analysis, that the computer owner has a reasonable expectation of privacy in her home or office,[53] which means the officers' entry into the premises constitutes a search under the Fourth Amendment. For such an entry to be lawful, it would have to be authorized either by a search warrant or by an applicable exception to the warrant requirement.[54] The same is true of the officers' "entry" into the computer. As such, I shall assume for the purposes of analysis that their accessing the contents of the computer-as-closed-container violates a reasonable expectation of privacy (again, absent countervailing circumstances)[55] and therefore must be authorized by a warrant or an exception to the warrant requirement.[56]

The analysis above applies to physical searches of someone's home or office and of a computer located in that home or office. Does it also apply to remote searches of computers located in a

---

remote searches targeting computers that are located in places other than the suspect's own home or office, e.g., in a home that belongs to someone other than the suspect or in a public place, such as an airport or a Starbucks. While computers located in someone's home or office may be entitled to a heightened level of Fourth Amendment protection, individuals do not necessarily surrender a reasonable expectation of privacy in a closed container by taking it with them into publicly accessible areas. *See, e.g.*, Bond v. United States, 529 U.S. 334, 336-37 (2000); *see also* United States v. Astley-Teixera, No. ACM 35161, 2003 WL 22495794, at *7 (A.F. Ct. Crim. App. Oct. 21, 2003) (defendant had a reasonable expectation of privacy in his laptop, which he left "open, powered-on, and not password protected" in his dorm room).

[53] Absent countervailing circumstances, individuals enjoy a reasonable expectation of privacy in their own homes. *See, e.g.*, Payton v. New York, 445 U.S. 573, 589-90 (1980). And, depending on the circumstances, individuals may have a reasonable expectation of privacy in their offices. *See, e.g.*, O'Connor v. Ortega, 480 U.S. 709, 715-17 (1987).

[54] *See supra* note 47 and accompanying text.

[55] For what constitutes such circumstances, see *infra* notes 58-60 and accompanying text.

[56] *See, e.g.*, United States v. Hanson, No. CR 09-00946 JSW, 2010 WL 2231796, at *3 (N.D. Cal. June 2, 2010).

home or office? To resolve that question, we need to analyze several distinct issues, the first of which is whether a remote computer search involves a physical "entry" of the home or office in which the computer is located. Literally, it does not; the officers who examine the contents of the computer's hard drive do not physically cross the threshold of the home or office in which it is located.[57] Logically, then, a remote computer search is a more circumscribed Fourth Amendment event than the traditional computer searches outlined above; in a remote search, the officers access the contents of the computer's hard drive but not the premises on which it is located. Arguably, they would not need to obtain a warrant to search those premises in order to conduct the remote search of the computer; since there is no physical entry into the home or office, it seems the only potential Fourth Amendment event is the exploration of the computer.[58]

As we saw earlier, absent countervailing circumstances, individuals will have a reasonable expectation of privacy in their computers—especially if they are located in generally private areas, such as a home or office—because computers are considered to be "closed containers."[59] Computers, though, differ from traditional containers in one notable respect: They are linked to the Internet through a network (which, of course, is essential if our hypothesized investigators are to conduct remote computer searches). To access traditional containers, law enforcement officers must cross the threshold of the suspect's home or office in order to locate and access the contents of the container; to access a networked computer, officers can exploit the fact that it is online. That adds a dimension to the analysis; the computer-container essentially offers officers a direct portal into the data it contains, a

---

[57] *See supra* note 53 and accompanying text.

[58] United States v. Martinez-Fuerte, 428 U.S. 543, 561 (1976). The absence of "[p]hysical entry of the home" in this scenario removes the "chief evil against which the . . . Fourth Amendment is directed." United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div., 407 U.S. 297, 313 (1972). The text below examines the related issue of whether the officers' copying data from the computer constitutes a Fourth Amendment seizure that must also be authorized by a warrant or an exception to the warrant requirement.

[59] *See supra* notes 49-50 and accompanying text.

point of "entry" they can exploit without affecting any physical entry into Fourth Amendment-protected premises.

Is the availability of that portal sufficient, in and of itself, to negate the reasonable expectation of privacy individuals would otherwise enjoy in their computer-containers? An argument can be made that it does: A number of courts have found that one who installs and enables "peer-to-peer file sharing on his computer, thereby giving anyone with internet access the ability to gain entrance to his computer," has "no reasonable expectation of privacy" in the contents of that computer.[60] These courts have held, therefore, that it is not a violation of the Fourth Amendment for a law enforcement officer to utilize file-sharing software to locate and download files designated for sharing from someone's computer, even if that computer was in the suspect's home.[61]

Prosecutors and law enforcement officers might argue that the same premise applies to computer users who link their computers to the Internet. As we saw earlier, to have a cognizable Fourth Amendment expectation of privacy in a place or thing, one must subjectively believe the place or thing is private, and society must accept that belief as objectively reasonable.[62] Courts have found that those who use file-sharing software do not have such an expectation of privacy as to the files they designate for sharing even if they personally believe the files are private because society does not accept that belief as objectively reasonable.[63] These courts have, at least implicitly, found that the use of file-sharing

---

[60] United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008); *see also* United States v. Stults, 575 F.3d 834, 842-43 (8th Cir. 2009). The premise is that by installing and using file-sharing software, the person "knowingly exposes to the public" information that would otherwise be protected by the Fourth Amendment. United States v. Norman, No. 2:09-CR-118-WKW, 2010 WL 3825606, at *4 (M.D. Ala. July 6, 2010), report and recommendation accepted in part, rejected in part, No. 2:09cr118-WKW, 2010 WL 3825601 (M.D. Ala. July 6, 2010).

[61] *See, e.g.*, United States v. Ladeau, No. 09-40021-FDS, 2010 WL 1427523, at *3-6 (D. Mass. Apr. 7, 2010).

[62] *See supra* note 44 and accompanying text.

[63] *See, e.g.*, United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008).

software defeats a Fourth Amendment expectation of privacy only as to the files the person has made available for sharing.[64]

In other words, they have not held that the mere act of linking a computer to a network (and thereby to the Internet) defeats the owner's reasonable expectation of privacy in the contents of the computer itself. Indeed, at least one court has held to the contrary.[65] That, I submit, is the correct way to approach Fourth Amendment privacy with regard to computers that are (merely) linked to a network. I believe this approach is consistent with the Supreme Court's decision in *Katz v. United States*.[66] The *Katz* Court held that it was a Fourth Amendment search for law enforcement officers to use "an electronic listening and recording device" to access and capture the contents of calls he made while in a public telephone booth.[67] The Court found that Charles Katz had a reasonable expectation of privacy in the contents of the calls because he subjectively believed they were private and society accepted his belief as objectively reasonable.[68]

It seems to me that the computer user whose hard drive is invaded by a law enforcement Trojan Horse program is in a situation functionally analogous to the one Katz found himself in. Both utilize methods of "online" communication that rely on technology; both assume their "content" is private—the computer user because she is on her computer in her home or office, and Katz because he was in a phone booth the door of which was securely closed.[69] In neither scenario can law enforcement access

---

[64] *Id.* ("Ganoe thus opened up his download folder to the world, including Agent Rochford."); *see also* United States v. Borowy, 577 F. Supp. 2d 1133, 1136 (D. Nev. 2008).

[65] *See* United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007) ("[T]he mere act of accessing a network does not in itself extinguish privacy expectations . . . .").

[66] 389 U.S. 347 (1967).

[67] *Id.* at 348, 359.

[68] *Id.* at 351-59*; see also id.* at 360-62 (Harlan, J., concurring).

[69] The scenarios differ in one respect: In *Katz*, the officers intercepted the contents of Katz's phone conversations as they occurred; in our hypothesized scenario, officers access content that is stored on the computer user's hard drive. I do not see this distinction as particularly significant for the present analysis because I think it is purely the product of empirical circumstance: Since phone conversations are dynamic, the only ways the officers could obtain the contents of Katz's calls was to record them as they occurred. Computer-stored content, on the other hand, is relatively stable,

the content in question without utilizing dedicated technology that lets the officers invade a private enclave (hard drive, phone booth) in a fashion a reasonable person would not expect. In neither scenario do we have the target of that invasion engaging in conduct that abrogates a Fourth Amendment expectation of privacy in the area that is invaded, i.e., neither Katz nor our hypothetical computer user knowingly engaged in conduct that exposed their respective content to the public, and thereby to law enforcement.

I will, therefore, assume that law enforcement's using a Trojan Horse program to surreptitiously obtain content from the hard drive of a computer in someone's home or office constitutes a Fourth Amendment search and must be authorized either by a search warrant or by an exception to the warrant requirement. That, of course, only generates additional questions: What should such a warrant contain? How is it to be executed? What exceptions might substitute for a warrant in this context?

I will address those issues in a moment. Before I proceed with that analysis, I want to briefly address the issue as to whether law enforcement's using a Trojan Horse program to download content from someone's hard drive constitutes a "seizure" under the Fourth Amendment.

D. Seizure

As I noted earlier, a seizure of property occurs when law enforcement conduct "meaningfully" interferes with the owner's possession and use of that property.[70] In this analysis, I am assuming officers use a Trojan Horse program to access the contents of an unwary computer user's hard drive (search), to copy

---

regardless of its nature; a hard drive can store user-generated content, content the user downloaded from the Internet and emails the user has exchanged with others. *See, e.g.*, Lincoln Spector, *Where Does Windows Live Mail Store My Mail?*, PC WORLD (Apr. 8, 2011, 7:11 AM), http://www.pcworld.com/article/223781/where_does_windows_live_mail_store_my_mail.html. I do not see the type of information being accessed as dispositive; what matters is that, in both scenarios, officers use surreptitious communications technology to obtain content they otherwise would not be able to obtain except by physically invading a Fourth Amendment space, e.g., the computer user's home/office or Katz's phone booth.

[70] *See supra* note 45 and accompanying text.

data from that hard drive and to retrieve the copy for the officers' professional use. To constitute a seizure, the acts of copying the data and retrieving the copy would have to "meaningfully" interfere with the owner of the data's ability to possess and use it.

As I have explained elsewhere, I believe copying data is a seizure, albeit a seizure that differs in one important respect from traditional seizures of property.[71] In a traditional seizure of physical property, an officer prevents the owner from accessing that property for a brief period of time (temporary detention) or permanently (by taking the property with no intention of returning it to the owner). Either type of physical seizure is a zero-sum event, i.e., the possession and use of the property passes wholly from the owner to the officer for the duration of the seizure. Copying data is, as I have argued elsewhere,[72] a non-zero-sum seizure, i.e., there is a less than absolute interference with the owner's possession and use of the property.

Assume FBI Agent John Doe uses a Trojan Horse program to access the hard drive of Mary Smith's computer, which is in her home. After searching the contents of the hard drive, Doe copies certain files and downloads the copies to his hard drive. Smith still has the data, but she no longer has exclusive possession of it; that, I argue, results in a meaningful interference with her possession of that property.[73]

I analogize this type of copying to copying that is prosecuted as theft. In 1993, Randal Schwartz was prosecuted for theft of proprietary information.[74] The prosecution was based on Schwartz's copying a computer password file that belonged to the

---

[71] *See* Susan W. Brenner & Barbara S. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39, 106-13 (2002); Susan W. Brenner, *Copying as Search and Seizure*, CYB3RCRIM3 (Oct. 26, 2009, 8:32 AM) [hereinafter Brenner, *Copying*], http://cyb3rcrim3.blogspot.com/2009/10/copying-as-search-and-seizure.html; Susan W. Brenner, *Seizure*, CYB3RCRIM3 (Feb. 19, 2006, 2:35 PM), http://cyb3rcrim3.blogspot.com/2006/02/seizure.html.

[72] *See* Brenner, *Copying*, *supra* note 71.

[73] *See* Brenner, *Copying*, *supra* note 71. For a case that reached a similar conclusion, see *United States v. Jefferson*, 571 F. Supp. 2d 696, 703-04 (E.D. Va. 2008) (photographing information constituted a seizure).

[74] State v. Schwartz, 21 P.3d 1128, 1131, 1135 (Or. Ct. App. 2001).

Intel Corporation, which had employed him as a contractor.[75] After being convicted, Schwartz appealed, arguing, in part, that he could not be convicted of "theft" because while he copied the password file, "the file and passwords remained on Intel's computers."[76] The prosecution argued, in response, that the "loss of exclusive possession of the passwords . . . [was] sufficient to constitute theft."[77] After parsing the meaning of "theft," the court of appeals concluded that it could encompass non-zero-sum appropriations of intangible property, and therefore upheld Schwartz's conviction.[78]

This court, therefore—at least implicitly—recognized that copying data constitutes a meaningful interference with the owner's possession and use of that digital property, even though it does not wholly deprive the owner of the possession of that property. If we extrapolate that principle to the Fourth Amendment context, I believe we necessarily conclude that copying is a non-zero-sum seizure.

For the purposes of this analysis, then, I will assume that law enforcement's copying data constitutes a seizure. That brings us to the next issue—ensuring that the use of a Trojan Horse program to carry out digital searches and seizures is reasonable.

E. Trojan Horse Warrants

A Trojan Horse warrant would have to be supported by probable cause,[79] i.e., would have to be based on facts and circumstances that are "sufficient . . . to warrant a man of reasonable caution in the belief that" evidence of a crime will be found in the computer to be searched.[80] Establishing probable cause to conduct a remote computer search should not be

---

[75] *Id.* at 1130-31.

[76] *Id.* at 1136.

[77] *Id.* at 1137.

[78] *See id.*

[79] *See* U.S. CONST. amend. IV ("[N]o Warrants shall issue, but upon probable cause . . . .").

[80] Brinegar v. United States, 338 U.S. 160, 175-76 (1949) (quoting Carroll v. United States, 267 U.S. 132, 162 (1925)) (internal quotation marks omitted); *see, e.g.*, Ornelas v. United States, 517 U.S. 690 (1996) (standard enunciated above constitutes probable cause to search for evidence).

particularly difficult. In *United States v. Gitarts*,[81] the FBI developed the information needed to establish probable cause for a "remote" search of a computer server by working with a confidential informant and obtaining information from other credible sources.[82] Officers have also used information concerning a suspect's use of file-sharing software to establish the probable cause needed to obtain a warrant to search a computer for child pornography.[83]

The warrant would also have to particularly describe "the place to be searched, and the . . . things to be seized."[84] The "place" to be searched is the suspect's computer. When officers obtain a warrant to conduct a traditional search of a suspect's computer, they may particularly describe that specific computer[85] or they may seek a warrant to the computer or computer to be found at the premises where the search is to be conducted. Since computers are regarded as "containers," courts have held that a warrant satisfies the Fourth Amendment if it authorizes a search of a computer or computers. Officers might employ these approaches in obtaining a warrant for a Trojan Horse search, or they might proceed somewhat differently. They might "particularly describe" the "place" to be searched as the computer that is using a specific internet protocol (IP) address.[86]

The "things to be seized" would consist of computer data. The warrant would have to describe the things to be searched for and seized with some specificity, which would probably be done by specifying the *type* of data the officers are authorized to seek and

---

[81] 341 F. App'x 935 (4th Cir. 2009).

[82] *See id.* at 937-39. The prosecution was brought in Virginia; the server was in Texas. *Id.* at 939.

[83] *See, e.g.*, Panuski v. State, No. 88, 2010, 2010 WL 3398945, at *1 (Del. Aug. 30, 2010); State of Delware's Answering Brief at *3-4, Panuski v. State, No. 88, 2010, 2010 WL 2565705 (Del. June 14, 2010).

[84] U.S. CONST. amend. IV.

[85] *See, e.g.*, United States v. Voraveth, Crim. No. 07-419 DWF/AJB, 2008 WL 4287293, at *3 (D. Minn. July 1, 2008).

[86] *See, e.g.*, United States v. Rosetter, Crim. No. 10-83 (JNE/JSM), 2010 WL 5184991, at *13-14 (D. Minn. Oct. 1, 2010); United States v. Klynsma, No. CR. 08-50145-RHB, 2009 WL 3147790, at *7 (D.S.D. Sept. 29, 2009); *see generally* Johnson v. Microsoft Corp., No. C06-0900RAJ, 2009 WL 1794400, at *3 (W.D. Wash. June 23, 2009) ("When a person uses a computer to accesses the Internet, the computer is assigned an IP address by the user's Internet service provider.").

acquire. Courts have held that the Fourth Amendment's particularity requirement is satisfied if officers "describe with particularity the objects of their search," e.g., specify they are searching for evidence of child pornography or evidence of drug dealing and seek authorization to seek that evidence if and when they find it.[87] So, a Trojan Horse warrant might specify that the malware is to be used to search a computer remotely for evidence of terrorist activity or child pornography.[88]

That brings us to executing the warrant. Given the nature of the search, it seems obvious that the officers who remotely access the computer will not knock and announce their intention to "enter" it to conduct the search.[89] Although the Supreme Court has held that knocking and announcing is an element of Fourth Amendment analysis,[90] officers are not required to knock and announce their presence and intentions if they have reasonable suspicion that doing so would be dangerous or would inhibit the investigation by giving a suspect the opportunity to destroy evidence.[91] It is highly unlikely that officers initiating a remote search of a suspect's computer would reasonably fear physical injury to themselves, but they might very well have reason to suspect that announcing their intentions prior to commencing the search could result in the destruction of evidence. If the officers charged with executing a specific Trojan Horse warrant could

---

[87] United States v. Welch, 291 F. App'x 193, 205 (10th Cir. 2008); *see also* United States v. Stabile, 633 F.3d 219, 237-39 (3d Cir. 2011); United States v. Blake, No. 1:08-cr-0284 OWW, 2010 WL 702958, at *3 (E.D. Cal. Feb. 25, 2010).

[88] Two authors have suggested that the Trojan Horse program might be configured so that it automatically avoids data that is not within the scope of the Trojan Horse warrant:

> If a police Trojan has accessed a suspect's computer and is searching the hard-drive for relevant data, it should "understand" that certain types of . . . private data such as health records, is protected by the constitutional rights of the suspect, and is therefore "inaccessible" by the police. This should trigger a corresponding "disability" by the agent to collect information unless there is also a superseding "power" that overrules the suspect's constitutional rights on this occasion, and allows the exceptional violation.

Abel & Schafer, *supra* note 21.

[89] *See, e.g.*, Wilson v. Arkansas, 514 U.S. 927, 930 (1995) (common-law knock-and-announce principle is part of Fourth Amendment reasonableness analysis).

[90] *Id.*

[91] *See* Richards v. Wisconsin, 520 U.S. 385, 394-95 (1997).

articulate the necessary reasonable suspicion, that should eliminate the need for virtual knocking and announcing; the process would, of course, proceed on a case-by-case basis.

The Fourth Amendment does not specify a time period within which warrants must be executed, but the federal system and most, if not all, states do this with court rules or statutes.[92] Under Rule 41 of the Federal Rules of Criminal Procedure, warrants that authorize copying "electronically stored information" are executed in a timely fashion if the information is copied within the specified time period.[93] This is a reasonable approach for the execution of what I am referring to as traditional computer searches, but it may not be adequate for Trojan Horse warrants.

Rule 41 and the comparable state provisions all assume that the "execution" of a warrant is a single, unitary event, analogous to officers' seizing stolen televisions from a suspect's home. That assumption is almost certainly not valid for Trojan Horse warrants because they are executed, not by human beings, but by semi-autonomous software programs. [94] Since Trojan Horse programs "can work autonomously without the direct intervention of a human controller, their search is not limited to a specific time period. Hence, they are (potentially) ubiquitous and 'always on.'"[95] Court rules and statutes could address this issue by requiring (i) that the Trojan Horse program be deleted from the target computer once the authorized search had been completed or (ii) that officers disable the program, thereby preventing it from continuing to conduct searches on the target computer.[96]

---

[92] *See, e.g.*, FED. R. CRIM. P. 41(e)(2)(A)(i) ("14 days"); *see also* ALA. CODE § 15-5-12 (1995); IDAHO CODE ANN. § 19-4412 (2004); W. VA. CODE ANN. § 62-1A-4 (LexisNexis 2010); 68 AM. JUR. 2D *Searches and Seizures* § 302 (2010).

[93] *See* FED. R. CRIM. P. 41(e)(2)(B). The rule is intended to clarify that a warrant for digital evidence is "executed" when the evidence is seized, not when the review of the evidence is complete. *Id.*

[94] *See* Abel & Schafer, *supra* note 21.

[95] *Id.*

[96] I am assuming, for the purposes of analysis, that the execution of a Trojan Horse warrant only targets content that was stored on the computer when the software was installed on it. That is, I am assuming the Trojan Horse program does *not* intercept content as it arrives and is stored on the computer. Intercepting content, especially communications such as e-mail, would implicate the heightened requirements of Title III and analogous state wiretap statutes. *See, e.g.*, U.S. Dep't of Justice Computer Crime and Intellectual Prop. Sec., *Searching and Seizing Computers and Obtaining*

I need to address one final issue that could complicate the execution of a Trojan Horse warrant before I address the use of exceptions to the warrant requirement as an alternative way of satisfying Fourth Amendment requirements for remote computer searches. That issue is the unique problem posed by antivirus software.

As one article notes, a police Trojan Horse program is "from a design perspective nothing else than a piece of malware," and antivirus software is designed to detect and deflect malware.[97] "The problem is that any government-designed [Trojan Horse program] features these attributes and may therefore be detected by anti-virus products because they are not able to differentiate between a" law enforcement program and malware.[98] Commercial antivirus software installed on the target computer could therefore interfere with, or even block, the law enforcement Trojan Horse's ability to conduct the search (and seizure) authorized by the warrant. Unless law enforcement could create (or acquire) Trojan Horse programs that were not detected by commercial antivirus software, the solution to this problem seems to lie in law enforcement's persuading antivirus companies to "deliberately not detect" law enforcement Trojan Horse programs or disable their antivirus software if and when such a program were installed pursuant to a warrant.[99] One problem with this solution is that it could cause consumers to lose trust in the products created and marketed by the cooperating antivirus vendors; another problem is the "companies that [create] antivirus software are not necessarily in the same jurisdiction as the suspect" whose computer is to be searched, which means the relevant antivirus

---

Electronic Evidence in Criminal Investigations: Electronic Surveillance in Communications Networks, CYBERCRIME.GOV (2009), http://www.cybercrime.gov/ssmanual/04ssma.html; *see also* State v. Poling, 938 N.E.2d 1118, 1124 (Hocking Cnty. Mun. Ct. 2010).

[97] Abel & Schafer, *supra* note 21.

[98] *Id.*

[99] *Id.* There are federal and state statutes that authorize law enforcement officers to utilize the assistance of private citizens in executing warrants. *See, e.g.*, 18 U.S.C. § 3105 (2006).

company or companies might have little, if any, incentive to cooperate with U.S. law enforcement. [100]

F. Exceptions

Since I suspect many of the exceptions to the Fourth Amendment's warrant requirement—such as search incident to arrest, inventory searches, consent searches, the vehicle exception and administrative searches—are likely to have little, if any, applicability to remote computer searches, I am only going to address two exceptions: one, which is likely to apply, and the other, which is not likely to apply in this context.

The exception that is likely to apply is the exigent circumstances exception. The exception allows officers to enter premises without a warrant to conduct a search if they have probable cause to conduct the search and if an exigency justifies entering without a warrant.[101] Courts have recognized four types of exigency that justify such an entry: (1) the need to prevent physical harm to someone inside the premises; (2) the need to prevent the imminent destruction of evidence; (3) hot pursuit of a fleeing suspect; and (4) the need to prevent the escape of a suspect.[102] I, for one, do not believe three of these exigencies could apply to remote computer searches; the only exigency I see that could apply here is the need to prevent the destruction of evidence.

There is, indeed, precedent for applying this exigency to a remote computer search. In *United States v. Gorshkov*, [103] FBI agents "logged onto" a computer in Russia that was used by a cybercrime suspect whom they had arrested. [104] The agents downloaded data from the Russian computer without first obtaining a warrant; the government later used the data in its prosecution of the suspect—Vasiliy Gorshkov.[105] Gorshkov moved to suppress the data, claiming the search of his computer violated

---

[100] Abel & Schafer, *supra* note 21.

[101] *See, e.g.*, United States v. Struckman, 603 F.3d 731, 739 (9th Cir. 2010).

[102] *Id.* at 743.

[103] No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001).

[104] *See id.* at *1.

[105] *Id.*

the Fourth Amendment.[106] The prosecution argued that the search was justified by the exigent circumstances exception because the "agents had probable cause to believe that the Russian computers contained evidence of crimes" and "good reason to fear that if they did not copy the data," Gorshkov's "coconspirators would destroy" it.[107] The district court agreed with the prosecution, and denied Gorshkov's motion to suppress.[108] I can see the same theory being used to justify remote computer searches, as long as the officers who are charged with carrying out the search can point to specific facts that reasonably led them to believe they needed to act without first obtaining a warrant.

The exception I do not believe can apply in this context is not really an exception at all. As the Supreme Court noted in *Texas v. Brown*,[109] the plain view doctrine "is perhaps better understood . . . not as an . . . 'exception' to the Warrant Clause, but . . . as an extension of whatever the prior justification for an officer's 'access to an object' may be."[110] Under the plain view doctrine, "if police are lawfully in a position from which they view an object, if its incriminating character is immediately apparent, and if the officers have a lawful right of access to the object, they may seize it without a warrant."[111] The doctrine only justifies a seizure; it cannot justify a search.[112]

Courts have upheld the applicability of the plain view doctrine in police-initiated physical searches of computers and hard drives.[113] Typically, courts uphold the applicability of the plain view doctrine when an officer is searching a computer's hard drive pursuant to a search warrant, observes data whose "incriminating character. . . [is] 'immediately apparent,'" and seizes the data.[114] I do not see how this dynamic can apply in remote computer searches because here the search is conducted,

---

106 *Id.*
107 *Id.* at *4.
108 *Id.*
109 460 U.S. 730 (1983).
110 *Id.* at 738-39.
111 Minnesota v. Dickerson, 508 U.S. 366, 375 (1993).
112 *See id.*
113 *See, e.g.*, United States v. Stabile, 633 F.3d 219, 240-41 (3d Cir. 2011).
114 *Id.* at 241.

not by a human being, but by semi-autonomous software.[115] There is, therefore, no individual to observe data the incriminating character of which is immediately apparent to him or her; absent that, how can the plain view doctrine apply?

Some might argue that software could be configured so the Trojan Horse program being used in the search could, like a human investigator, recognize data that was not within the scope of the warrant but that was clearly incriminating for different reasons, and that it would be reasonable to allow the software to expand its activities by merely seizing this evidence, as well. Aside from anything else, I, for one, would be reluctant to allow this expansion of the plain view doctrine for fear that it might lead to manipulations that deliberately and impermissibly expanded the scope of a Trojan Horse warrant.

II. VIRTUAL FORCE?

In November 2010, WikiLeaks, a "whistleblower" organization used the Internet to publish "[a] cache of a quarter-million confidential" diplomatic cables from 274 United States embassies.[116] WikiLeaks apparently received the cables from Bradley Manning, a U.S. Army soldier who allegedly downloaded them from SIPRNet, the Secret Internet Protocol Router Network used by the U.S. Department of Defense and Department of State.[117]

As WikiLeaks began releasing the cables, the computer servers that hosted its website were attacked by unknown sources, taking the website offline.[118] The attack took the form of a Distributed Denial of Service (DDoS) attack,[119] which overwhelms

---

[115] *See* Abel & Schafer, *supra* note 21.

[116] Scott Shane & Andrew W. Lehren, *Leaked Cables Offer Raw Look at U.S. Diplomacy*, N.Y. TIMES, Nov. 29, 2010, at A1, *available at* http://www.nytimes.com/2010/11/29/world/29cables.html.

[117] *See, e.g.*, Kim Zetter, *Army: Manning Snuck 'Data-Mining' Software Onto Secret Network*, WIRED (Apr. 4, 2011, 4:28 PM), *available at* http://www.wired.com/threatlevel/2011/04/manning-data-mining/.

[118] *See, e.g.*, *WikiLeaks Under Denial of Service Attack (DDoS)*, SECURITY WEEK (Nov. 28, 2010), http://www.securityweek.com/wikileaks-under-denial-service-attack-ddos.

[119] *Id.* ("[I]ts Web site is currently under mass distributed denial of service attack.").

a website with so much traffic it becomes "unavailable to its intended users."[120] A DDoS attack saturates the server hosting a website "with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable."[121] Cybercriminals often use DDoS attacks to extort money; the extortionists use a DDoS attack to shut down a commercial website, such as a casino, then demand money to refrain from repeating the attack.[122]

The DDoS attack against WikiLeaks was not designed to further an extortion attempt. It was apparently intended to impede WikiLeaks' ability to release the cables Manning allegedly leaked, which led some to suggest that the U.S. government was responsible for them.[123] In early December, a "Pentagon spokesman" said the U.S. Cyber Command[124] "had the means to shut down WikiLeaks but . . . policy makers thought it 'not appropriate' because [the] threat [was] not 'of high consequence.'"[125]

---

[120] Jason Fritz, *How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness*, 8 CULTURE MANDALA 28, 53 (2008), *available at* http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1110&context=cm.

[121] U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION STAFF REPORT: THE NATIONAL SECURITY IMPLICATIONS OF INVESTMENTS AND PRODUCTS FROM THE PEOPLE'S REPUBLIC OF CHINA IN THE TELECOMMUNICATIONS SECTOR 82-83 (2011), *available at* http://www.uscc.gov/RFP/2011/FINALREPORT_TheNationalSecurityImplicationsofInvestmentsandProductsfromThePRCintheTelecommunicationsSector.pdf.

[122] *See, e.g.*, John Leyden, *Korean Web Host Charged Over DDoS Extortion Scam*, REGISTER (Jan. 11, 2011, 12:28 GMT), http://www.theregister.co.uk/2011/01/11/korean_gambling_ddos_extortion_charges/.

[123] *See, e.g.*, Rob Korczak, *DDoS Attack on Wikileaks Failed to Stop Cablegate Leaks*, ASSOCIATED CONTENT (Nov. 28, 2010), http://www.associatedcontent.com/article/6064458/ddos_attack_on_wikileaks_failed_to_pg2.html?cat=15.

[124] The U.S. Cyber Command is a "sub-unified command subordinate to United States Strategic Command" that "centralizes direction of cyberspace operations," including offensive and defensive cyber-attacks. *U. S. Cyber Command*, UNITED STATES STRATEGIC COMMAND, http://www.stratcom.mil/factsheets/cyber_command/ (last visited Feb. 28, 2012).

[125] James Joyner, *Pentagon: We Could Have Taken WikiLeaks Down*, OUTSIDE THE BELTWAY (Dec. 2, 2010), http://www.outsidethebeltway.com/pentagon-we-could-have-taken-wikileaks-down/. Around the same time, a "self-proclaimed 'hacktivist'" said he was responsible for the attack. Paul McDougall, *"Hacktivist" Claims Credit for WikiLeaks Attack*, INFORMATIONWEEK (Dec. 1, 2010, 8:00 AM),

When I read about the WikiLeaks DDoS attack, it occurred to me that it might be coming from the U.S. government, which clearly had the motive and means to carry out such an assault. The idea of using DDoS attacks to shut down websites that host objectionable content is far from new: In 2001, then German Interior Minister Otto Schily "suggested that the German government" might use DDoS attacks "to shut down some sites based in the United States."[126] The sites in question were neo-Nazi websites, which provide content that is easily accessible in Germany; disseminating such content is a crime under German law.[127] Germany, of course, never launched such attacks; I suspect Schily's suggestion was simply the product of an understandable frustration at being unable to persuade U.S. authorities to block the sites or otherwise prevent the content they provide from being available to German citizens.

While the U.S. government may not have been responsible for the DDoS attack against WikiLeaks, this does not mean it cannot, and will not, use such attacks in the future. If the remarks of the "Pentagon spokesman" were reported correctly, the U.S. did not launch a DDoS attack against WikiLeaks because it did not deem the "harm" being inflicted by the release of the confidential (but not classified) cables significant enough to warrant such a response. It is therefore logical to infer that the United States *will* use a DDoS attack—or DDos attacks—to respond to the release of information or to other activity that inflicts "harm" significant enough to justify such a response. The likelihood of the United States resorting to DDoS attacks probably increases in proportion to the egregiousness of the "harm" being inflicted and the unavailability of alternative remedies.

The U.S. government's use of DDoS attacks to respond to "harm" being inflicted by online activity raises a number of legal issues, including the possibility that the attacks could be

---

http://www.informationweek.com/news/cloud-computing/software/showArticle.jhtml?articleID=228400244.

[126] Steve Kettmann, *Nebraksa Neo-Nazi Irks German Pol*, WIRED (Jan. 10, 2002), http://www.wired.com/politics/law/news/2002/01/49566.

[127] *See* STRAFGESETZBUCH [StGB] [PENAL CODE] Nov. 13, 1998, BUNDESGESETZBLATT [BGBL. I] 3322, as amended, §§ 86 & 86a (Ger.).

construed as offensive cyber-warfare.[128] That, however, is not the only possibility: Since warfare has traditionally involved a conflict between nation-states, the U.S. could argue that its using DDoS attacks against a civilian target constituted an exercise of law enforcement authority, rather than a military assault on another sovereign.[129] This argument is the product of what seems to have been a heretofore unrealized possibility: that a nation-state could use what in other circumstances would be military force against a civilian or group of civilians, the activities of which were in no way sponsored by or associated with the interests of a nation-state.[130]

If the use of DDoS attacks against a civilian target—a website that is disseminating classified information or bombarding U.S. targets with computer worms or other damaging data—represented an exercise of domestic law enforcement authority, the use of such attacks would have to comport with the requirements of the Fourth Amendment. That is the issue—the only issue—I will address in the remainder of this Article.[131]

To analyze the Fourth Amendment implications of using DDoS attacks against a civilian target that is located outside the United States, we need to outline a scenario that can provide the basis of our analysis and parse the Fourth Amendment principles that would be implicated by such an attack. For the scenario, we will use a variation of the WikiLeaks case. We will assume that a website located in another country is inflicting "harm" in the United States; the "harm" could involve releasing classified information, but I prefer to focus on something more concrete. We will assume that (i) the external site is attacking U.S. financial institutions; (ii) the attacks erode the stability of the institutions by interfering with normal operations and siphoning money from them; and (iii) the U.S. has asked the government of the country

---

[128] *See, e.g.*, SUSAN W. BRENNER, CYBERTHREATS: THE EMERGING FAULT LINES OF THE NATION STATE 65-70 (2009) [hereinafter BRENNER, CYBERTHREATS]. Since the attacks target computers and servers located in the territory of another nation-state, they could be analogized to the Japanese bombing of Pearl Harbor or Hitler's invading Poland. *See id.*

[129] *Id.*

[130] *See, e.g.*, BRENNER, CYBERTHREATS, *supra* note 128, at 235-38; *see generally id.* at 105-09.

[131] For an analysis of the cyberwarfare issues, see *id.* at 65-70.

in which the site is located for assistance in stopping the attacks and apprehending the perpetrators, but the government has refused to intervene.

Since the attacks target civilian entities, the responsibility for responding to them lies with civilian law enforcement. We will assume the FBI takes the lead in dealing with this situation. We will also assume that the FBI decides the best way to respond to the "harm" being inflicted by the external site is to use DDoS attacks to shut the site down.

The legal issue we then need to address is whether using DDoS attacks to shut down an external website implicates the Fourth Amendment. It presumably does not: The Supreme Court has held that the Fourth Amendment protects "the people of the United States against arbitrary action by their own Government," but in no way "restrain[s] the Federal Government's actions against aliens outside United States territory."[132] And in *United States v. Gorshkov,* a federal judge held that FBI agents do not violate the Fourth Amendment by accessing a Russian computer and downloading data without being authorized to do so.[133]

We could end this analysis by deciding there is no need to address the Fourth Amendment implications of using DDoS attacks against an external website. That is probably what a court would do. However, I think it is useful to proceed by considering how the Fourth Amendment *could* apply to actions taken in the virtual world of cyberspace. I think such a consideration is a useful exercise because U.S. courts may well find it necessary to revise the interpretation that limits the applicability of the Fourth Amendment to extraterritorial actions, at least when those actions involve the use of cyberspace.[134]

---

[132] United States v. Verdugo-Urquidez, 494 U.S. 259, 260 (1990); *see supra* note 41 and accompanying text.

[133] *See supra* notes 107-08 and accompanying text. As noted earlier, the judge held that the FBI's actions were justified by the exigent circumstances exception to the Fourth Amendment's warrant requirement. United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *4 (W.D. Wash. May 23, 2001). He also held that the Fourth Amendment did not apply to the FBI agents' actions because the Russian computer was not in the United States and was not owned by a U.S. citizen. *See id.* at *3.

[134] Aside from other considerations, courts may decide to revise the rule because of the tensions it can cause with other countries. *See, e.g.*, Mike Brunker, *FBI Agent*

We will assume, for the purposes of analysis, that the Fourth Amendment *can* (but does not necessarily) apply to the use of DDoS attacks to shut down an external target that is inflicting "harm" on U.S. citizens.

For the Fourth Amendment to apply to such activity, it must involve a "search" or a "seizure." Since DDoS attacks do not involve accessing—hacking into—the target computers, it does not seem that our hypothesized retaliation would involve a search. That leaves a seizure as the only remaining option. In *U.S. v. Jacobsen*, the Supreme Court held that a seizure of property occurs when "there is some meaningful interference with an individual's possessory interest in that property."[135]

For the purposes of analysis, we will assume that the external website is "property" and is owned by an individual—Mr. X. For a U.S.-launched DDoS attack on the website to constitute a seizure, it would have to meaningfully interfere with Mr. X.'s possessory interest in that site. Since the value—the utility—of a website lies in its functionality, it is logical to assume that shutting down Mr. X's website would interfere with his possessory interest in that property.[136]

The next question is whether the seizure of the website would be reasonable.[137] To be reasonable, the seizure would have to be conducted pursuant to a warrant or to a valid exception to the warrant requirement.[138] If the FBI has time to obtain a warrant, this would be the preferable approach to ensuring that the seizure satisfies the requirements of the Fourth Amendment. If, as seems

---

Charged With Hacking, MSNBC (Aug. 15, 2002), http://www.msnbc.msn.com/id/3078784/ns/news-internet_underground/.

[135] 466 U.S. 109, 113 (1984) (footnote omitted).

[136] Federal courts have held, for example, that an officer's killing someone's dog constitutes a Fourth Amendment seizure. *See, e.g.*, Brown v. Muhlenberg, 269 F.3d 205, 210 (3d Cir. 2001). Since a DDoS attack does not permanently take a website offline, it would not constitute this type of absolute seizure, i.e., a complete deprivation of the property, but would constitute a meaningful "interference" with the property.

[137] *See, e.g.*, United States v. Ramirez, 523 U.S. 65, 71 (1998) ("The general touchstone of reasonableness which governs Fourth Amendment analysis . . ." encompasses damage to property.).

[138] *See, e.g.*, Menotti v. City of Seattle, 409 F.3d 1113, 1154 (9th Cir. 2005). Warrants can authorize the use of force. *See, e.g.*, United States v. Husband, 226 F.3d 626, 639-40 (7th Cir. 2000).

more likely, the FBI decides it does not have time to get a warrant but must act quickly, then the agents could presumably rely on the exigent circumstances exception to the warrant requirement as justifying the DDoS attack.[139]

What might be involved in obtaining a DDoS warrant? The FBI agents would have to show they had probable cause to believe the seizure (the DDoS attack) was necessary to prevent and/or interrupt the commission of a federal crime and would have to particularly describe the target of the attack, i.e., Mr. X's website. They could no doubt use methods analogous to those described above, in the discussion of Trojan Horse warrants, to establish both. And, as with a Trojan Horse warrant, the DDoS warrant might also specify the time period for which the attack could be sustained and/or resumed if and when it was terminated or interrupted.[140]

The DDoS attacks might only be an interim measure—essentially, a cyber-*Terry* stop of a website. Since it would be difficult, if not impossible, to use DDoS attacks to take Mr. X's site permanently offline, the agents might want to resort to other types of cyber-force to accomplish that goal. They might, for example, want to use computer viruses or worms to destroy the site, which of course would require parsing the requirements for the use of those cyber-weapons and using the relevant Fourth Amendment principles to authorize their use.

CONCLUSION

When I finished the initial draft of this article in the early spring of 2011, the tactics analyzed above both were (at least as far as I knew) still mere possibilities. In April, 2011, the Department of Justice and the FBI launched a joint effort to take down a massive Coreflood botnet.[141]

---

[139] *See* United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *4 (W.D. Wash. May 23, 2001).

[140] When the attack(s) finally ended, the agents could return it, together with a description of what was done to execute it, to the magistrate who issued it. *See* FED. R. CRIM. P. 41(f)(1)(D).

[141] As an FBI press release explained:

As part of that effort, the Department of Justice sought and obtained a temporary restraining order from a federal judge in Connecticut that let a nonprofit entity, working "under law enforcement supervision," seize and replace computer servers being used to operate the botnet with servers controlled by it and by the FBI.[142] The Justice Department's initial filing with the court also noted that this entity, again working "under law enforcement supervision," would "collect the IP addresses of all infected machines communicating with the criminal servers, and send a remote 'stop' command to infected machines to disable the Coreflood malware operating on them."[143]

In the Memorandum of Law the Department of Justice submitted in support of its request for the temporary restraining order, the Department argued that "stop[ping] the Coreflood virus" did not constitute either a search or a seizure under the Fourth Amendment.[144] According to the memorandum, there would be "no cognizable 'search' under the Fourth Amendment" because the government was not seeking authorization to "obtain or record any data that [was] on the infected computers."[145] It also argued that there was no seizure because the steps taken to stop the Coreflood infection would not "meaningfully interfere with a

---

> Botnets are networks of virus-infected computers controlled remotely by an attacker. They can be used to steal funds, hijack identities, and commit other crimes. The botnet in this case involves the . . . Coreflood virus, a key-logging program that allows cyber thieves to steal personal and financial information by recording unsuspecting users' every keystroke. Once a computer or network of computers is infected by Coreflood—infection may occur when users open a malicious e-mail attachment—thieves control the malware through remote servers.

Botnet Operation Disabled, FED. BUREAU OF INVESTIGATION (Apr. 14, 2011), http://www.fbi.gov/news/stories/2011/april/botnet_041411.

[142] Kim Zetter, *With Court Order, FBI Hijacks "Coreflood" Botnet, Sends Kill Signal*, WIRED (Apr. 13, 2011, 6:17 PM), http://www.wired.com/threatlevel/2011/04/coreflood/.

[143] *Id.*; *see supra* note 86 and accompanying text.

[144] *See* Government's Memorandum of Law in Support of Motion for Temporary Restraining Order, Preliminary Injunction, and Other Ancillary Relief at 46, United States v. John Doe, No. 3:11 CV 561 (VLB) (D. Conn. Apr. 12, 2011), *available at* http://www.steptoe.com/assets/attachments/4253.pdf.

[145] *Id.* at 46.

computer owner's possessory interests over an infected computer."[146]

As noted above, the Connecticut district court granted the temporary restraining order; eleven days later, the Department of Justice returned to the court, this time asking that the temporary restraining order "be continued as a preliminary injunction."[147] The memorandum submitted in support of this request asked that the authorization provided by the temporary restraining order be continued to allow the remediation efforts undertaken under the original order to continue; it noted that the efforts had significantly reduced the size of the Coreflood botnet, and should continue to do so if the authorization remained in effect.[148]

It also noted that the government intended to begin uninstalling Coreflood "from the computers of Identifiable Victims who provide written consent" to such measures.[149] In what was presumably an acknowledgment of the potential Fourth Amendment implications of such activity, the memorandum explained that the government was "not requesting explicit authorization from the Court" to initiate the uninstallation effort "because the written consent form obviates the need for such authorization."[150] As I write this, the court has not ruled on this request, but I will not be surprised if it is granted.

The U.S. government's 2011 initiative against the Coreflood botnet did not involve the use of Trojan Horse warrants, but I would argue that at least one aspect of it—the process of uninstalling the Coreflood virus from infected computers—involved the use of virtual force. The force was not directed at humans, but at a tool—or a weapon—cybercriminals were using to victimize U.S. citizens, among others. We can analogize "entering" the infected computers to eliminate the virus to scenarios in which

---

[146] *Id.* at 47. The memorandum also argued that eliminating the Coreflood virus from the computers did not constitute a seizure because the virus was an "instrumentality of crime," analogous to contraband. *Id.* at 51.

[147] Government's Supplemental Memorandum In Support of Preliminary Injunction at 15, United States v. John Doe, No. 3:11 CV 561 (VLB) (D. Conn. Apr. 23, 2011), *available at* http://www.justice.gov/opa/documents/coreflood-govt-supp.pdf.

[148] *Id.* at 9-15.

[149] *Id.* at 12.

[150] *Id.* at 12-13.

law enforcement officers physically enter premises to disable an explosive device and/or disarm someone who is holding victims hostage. One scenario involves the use of physical force in a physical environment; the other involves the use of virtual force in a virtual environment. The scenarios obviously differ in certain empirical respects, but I, for one, would argue that the conduct at issue is functionally analogous, at least as far as the Fourth Amendment is concerned.

I may be wrong, but I suspect we will see more law enforcement activity moving into the virtual world. If I am correct in that suspicion, then we should see other uses of virtual force and the use of Trojan Horse warrants, along with other virtual analogues of the tactics law enforcement officers have traditionally used in the physical world.