NEW YORK LAW SCHOOL

NYLS Law Review
Vols. 22-63 (1976-2019)

Volume 49
Issue 1 *State of Play*

Article 16

January 2004

United States v. Jarrett

Andres A. Munoz
New York Law School

Follow this and additional works at: https://digitalcommons.nyls.edu/nyls_law_review

 Part of the Criminal Law Commons, and the Internet Law Commons

Recommended Citation

Andres A. Munoz, *United States v. Jarrett*, 49 N.Y.L. SCH. L. REV. (2004-2005).

This Notes and Comments is brought to you for free and open access by DigitalCommons@NYLS. It has been accepted for inclusion in NYLS Law Review by an authorized editor of DigitalCommons@NYLS.

UNITED STATES v. JARRETT
(decided July 29, 2003)

ANDRES A. MUÑOZ*

Hackers[1] are routinely portrayed as super-criminals with extraordinary powers who roam the internet in search of valuable information contained within a person's or a company's computers.[2] But, what happens when a hacker stumbles across information that may incriminate its owner? How does the law define when the government is able to use information that a hacker has decided to turn over to law enforcement? Until recently, courts have not faced such questions; however, with the proliferation of the Internet and computer networks, courts now face the challenge of applying conventional law to cutting-edge technological issues.[3]

In *United States v. Jarrett*, the Fourth Circuit faced one such challenge.[4] In *Jarrett*, the issue was whether the prosecution could use information obtained from a private hacker's search of the defendant's personal computer. The court, in analyzing the issue of suppression, looked at whether an agency relationship existed between the government and the hacker and applied a traditional two-part agency relationship test to an ultra-modern problem to produce a flawed result. Instead of requiring that the government actively acquiesce in a search to establish the agency relationship, the court should have only looked to see if there was passive acqui-

* J.D. Candidate 2005, New York Law School.

1. In this context, a hacker is defined as "One who uses programming skills to gain illegal access to a computer network or file." THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 545 (4th ed. 2000).

2. Michael Lee et al., Comment, *Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal*, 14 BERKELEY TECH. L.J. 839, 845 (1999).

3. *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) (recognizing that courts have struggled to analyze problems involving modern technology within the confines of the Electronic Communications Privacy Act); *see also* Michelle R. Jackson-Carter, Note and Comment, *International Shoe and Cyberspace: The Shoe Doesn't Fit When It Comes to the Intricacies and Nuances of Cyberworld*, 20 WHITTIER L. REV. 217 (1998) (quoting Richard S. Zembek, Comment, *Jurisdiction and the Internet: Fundamental Fairness in the Networked World of Cyberspace*, 6 ALB. L.J. SCI. & TECH. 339, 342 (1996)) (acknowledging that courts have been struggling with jurisdictional issues in cyber-actions).

4. United States v. Jarrett, 338 F.3d 339 (4th Cir. 2003).

escence. Such a strict standard is needed to adequately protect a person's Fourth Amendment rights against unreasonable searches and seizures when dealing with hackers who turn over incriminating information to the government.

On July 16, 2000, a computer hacker, known as Unknownuser, contacted the Alabama Police Department with information regarding a Dr. Bradley Steiger.[5] Unknownuser, a citizen and resident of Istanbul, Turkey, hacked into Steiger's computer and found evidence of child pornography.[6] Unknownuser sent Captain Kevin Murphy of the Alabama Police Department an unsolicited email containing several of the images he found along with a text message in which Unknownuser explained that he had Steiger's personal information and additional pictures.[7] He then inquired whether he should send the information to the same email address.[8] Murphy's reply email stated, "Please feel free to send the information that you have. We will do everything we can."[9] After a series of emails, Unknownuser subsequently provided Murphy with Steiger's personal information, which was forwarded to FBI Agent Margaret Faulkner, who had a fixed working relationship with the Alabama Police Department regarding internet child pornography cases.[10] Using this information, the FBI identified and arrested Steiger and a jury convicted him of violating various federal statutes.[11] Steiger was sentenced to 17½ years imprisonment.[12] After the conviction, an FBI agent named Duffy, sent Unknownuser an email expressing his gratitude and saying that Unknownuser would not be prosecuted for hacking because, as a foreigner, he was not subject to U.S.

5. United States v. Jarrett, 229 F. Supp. 2d 503, 505 (E.D. Va. 2002).
6. *Id.*
7. *Id.*
8. *Id.*
9. *Id.* at 506.
10. *Id.* at 505.
11. *Jarrett*, 338 F.3d at 341.
12. United States v. Steiger, 318 F.3d 1039, 1045 n.1 (11th Cir. 2003).

laws.[13] The email also specified, "If you want to bring other information forward, I am available."[14]

A year after Agent Duffy's email, Unknownuser contacted Captain Murphy with information regarding another suspected child pornographer, William Jarrett.[15] Again, Unknownuser used hacking as the method to obtain information from Jarrett's personal computer.[16] Murphy instructed Unknownuser to send all information to Murphy's email address so that he could forward it to the FBI.[17] Through a total of thirteen emails, "including a ten-part series of emails with a total of 45 attached files," Unknownuser provided the FBI with all the evidence of child pornography and personal information necessary to produce an arrest.[18] After the arrest, Agent Faulkner sent Unknownuser an email thanking him for his assistance and then "engaged in what can only be characterized as the proverbial wink and a nod."[19] For the next two months, Unknownuser engaged in "pen-pal type correspondence" with Agent Faulkner.[20] In these emails, Faulkner expressed gratitude and admiration for Unknownuser and assured him that he would not be a target of law enforcement for his hacking activities.[21] Additionally, Unknownuser spoke freely of his hacking adventures and suggested in no uncertain terms that he would continue to search for child pornographers using the same methods employed to identify Steiger and Jarrett.[22]

13. *Jarrett*, 229 F. Supp. 2d at 509. This e-mail was also part of an unsuccessful FBI attempt to identify Unknownuser. FBI Agents Duffy and Faulkner, through the use of telephone calls and e-mails, encouraged Unknownuser to identify himself and possibly testify at Steiger's trial. Both agents repeatedly promised Unknownuser that he would not be arrested. *Id.*

14. *Id.*

15. *Jarrett*, 338 F.3d at 341-42.

16. *Jarrett*, 229 F. Supp. 2d at 510.

17. *Jarrett*, 338 F.3d at 342.

18. *Jarrett*, 229 F. Supp. 2d at 510.

19. *Jarrett*, 338 F.3d at 343. This proverbial wink and a nod consisted of the following statement: "I cannot ask you to search out cases such as the ones you have sent us . . . but if you should happen across such pictures as the ones you have sent us and wish us to look into the matter, please feel free to send them to us . . . We also have no desire to charge you with hacking . . .." *Id.*

20. *Id.*

21. *Id.*

22. *Id.*

Three weeks after Jarrett's arrest, a grand jury indicted him on one count of manufacturing child pornography in violation of 18 U.S.C.A. § 2251(a) and seven counts of receiving child pornography in violation of 18 U.S.C.A. § 2251(a)(2)(A).[23] Jarrett moved to suppress the evidence obtained through the execution of the search warrant on the ground that the government violated his Fourth Amendment rights in using the information provided by Unknownuser to secure the search warrant.[24] The district court denied the motion and Jarrett then entered a conditional guilty plea to a one-count criminal indictment charging him with manufacturing child pornography.[25] Prior to sentencing, however, Jarrett moved to reconsider his earlier motion to suppress on the basis of new evidence — the post-arrest series of emails exchanged between Unknownuser and Agent Faulkner.[26] The government did not disclose these emails until after Jarrett had entered his guilty plea.[27] The district court, after reviewing the series of emails between Unknownuser and FBI agents, concluded that an agency relationship had been established between the hacker and the government and that the government knew of and acquiesced in the searches conducted by Unknownuser and granted the defendant's motion to suppress the evidence.[28]

The district court began its legal analysis by reviewing the relevant case law and stated that there are particular factors, such as government knowledge, government presence during a search, and the government's failure to prevent a search, that, when standing alone, fail to establish the requisite agency relationship.[29] When looking at the case at bar, however the court held that there are many "individual factors in combination which, when viewed in their totality, show that the government and Unknownuser expressed their consent to an agency relationship."[30] While Unknownuser may have acted without government suggestion in

23. *Id.* at 342.
24. *Id.*
25. *Jarrett*, 338 F.3d at 342.
26. *Id.*
27. *Id.*
28. *Id.* at 343.
29. *Jarrett*, 229 F. Supp. 2d at 518-19.
30. *Id.* at 519.

the *Steiger* case, the same was not true for the search of Jarrett's computer.[31] The Duffy communications, the district court held, contained significant encouragement from law enforcement officers, specific requests to further assist the police with the investigation of Steiger, assurances that the information Unknownuser revealed was valuable to law enforcement and had helped save lives, requests to maintain future contact with law enforcement officers, and assurances that Unknownuser would not be prosecuted.[32] Therefore, the Duffy communications clearly showed that Unknownuser had established an agency relationship with the government after the Steiger matter; by the time Unknownuser was hacking into Jarrett's computer, there was far more than knowledge on the government's part.[33] As for the post-arrest Faulkner communications, the district court stated that "although the statements were made after Jarrett's arrest, they helped clarify the relationship between the government and Unknownuser."[34] The district court concluded that the government knew of and acquiesced in the Jarrett search and that Unknownuser's actions were motivated solely by an interest to further law enforcement efforts.[35] Thus, Jarrett's Fourth Amendment rights were violated.[36]

The Fourth Circuit reversed.[37] Writing for the court, Justice Motz reviewed the facts surrounding the *Steiger* case as well as the *Jarrett* case before stating that, in considering the suppression ruling, the court would review the district court's factual findings for clear error and its legal determinations *de novo*.[38] The court held that although the Fourth Amendment protects against unreasonable searches and seizures by government officials and those private individuals acting as agents of the government, it does not afford any protections when those searches are conducted by a private

31. *Id.* at 518-19.
32. *Id.*
33. *Id.*
34. *Id.* at 514.
35. *Jarrett*, 229 F. Supp. 2d at 519.
36. *Id.* at 519-20.
37. *Jarrett*, 338 F.3d at 348.
38. *Id.* at 343-44.

party.[39] Any such private wrongdoing does not deprive the government of the right to use evidence that it has acquired lawfully.[40]

To determine if an agency relationship exists, the court held one must look at the facts and circumstances surrounding each case and determine the degree of the government's participation in the private party's activities.[41] Such a determination involves looking at two primary factors: (1) whether the government knew of and acquiesced in the private search; and (2) whether the private individual intended to assist law enforcement or had some other independent motivation.[42] The court acknowledged that in prior decisions the Fourth Circuit had compressed this two-part test into "one highly pertinent consideration."[43] When determining whether the government acquiesced, the court stated that there must be some evidence of government participation either through initiating or instigating the private action; mere knowledge and passive acquiescence is not enough.[44] Here, the government conceded the existence of the second primary factor — that Unknownuser's motives stemmed from his interest in assisting law enforcement.[45] Thus, the court looked solely at whether the Government knew of and acquiesced in Unknownuser's search in a manner sufficient to transform Unknownuser into an agent of the government, and so render the search unconstitutional.[46]

The Fourth Circuit held that the district court erred in relying on the Unknownuser/Agent Faulkner exchanges to find that the government knew of and acquiesced in the Jarrett search.[47] While the emails between Unknownuser and Agent Faulkner established an ongoing relationship sufficient to make Unknownuser an agent

39. *Id.* at 344.

40. *Id.*

41. *Id.*

42. *Id.* at 348.

43. *Jarrett*, 338 F.3d at 345. This "one highly pertinent consideration is 'whether the government knew of and acquiesced in the intrusive conduct and whether the private party's purpose for conducting the search was to assist law enforcement efforts and further her own ends.' " *Id.* (quoting United States v. Feffer, 831 F.2d 734, 739 (7th Cir. 1987)).

44. *Jarrett*, 338 F.3d at 345.

45. *Id.* at 345.

46. *Id.*

47. *Id.*

of the government, the email exchanges "took place after Unknownuser had hacked into Jarrett's computer, after the fruits of Unknownuser's hacking had been made available to the FBI, after Jarrett's home and computer had been searched, and after Jarrett himself had been arrested."[48] Thus, the government's knowledge and acquiescence was entirely post-search and was irrelevant.[49] As for the emails between Unknownuser and Agent Duffy regarding the *Steiger* case, the court concluded that they were nothing more than "perfunctory expressions of gratitude for Unknownuser's assistance, assurances that Unknownuser would not be prosecuted, and a vague offer of availability to receive more information in the future."[50] The court then concluded by stating that without more evidence, these exchanges were not enough to create an agency relationship that would include the Jarrett search.[51] If the Duffy communications created such an agency relationship, "virtually any government expression of gratitude for assistance well prior to an investigation would effectively transform any subsequent search by the party into a government search."[52]

One important lesson thus emerges from *Jarrett*: so long as the government does not explicitly request hackers to search, hackers have the green light to search a person's computer for incriminating information and transmit it to law enforcement. This leads to the rather disturbing conclusion that only in the most blatant instances of government participation in an investigation will evidence obtained from a hacker be suppressed. Such a standard fails to take into account the unique nature of hacking.

Critical to both the court of appeals' and the district court's analysis was the degree of the government's acquiescence in the Jarrett search. Both courts, relying on well-settled precedent,[53] held that acquiescence requires some degree of active participation; mere passive acquiescence is insufficient to produce a Fourth

48. *Jarrett*, 338 F.3d at 345.
49. *Id.* at 346.
50. *Id.*
51. *Id.*
52. *Id.*
53. *See* United States v. Ellyson, 326 F.3d 522 (4th Cir. 2003) (holding that acquiescence requires some degree of active government participation); United States v. Koenig, 856 F.2d 843 (7th Cir. 1988) (same); United States v. Walther, 652 F.2d 788 (9th Cir. 1981) (same); United States v. Smythe, 84 F.3d 1240 (10th Cir. 1996) (same).

Amendment violation.[54] In support of this proposition, the court of appeals stated, "it is only by the exercise of some form of control that the actions of one may be attributed to another."[55] "Mere knowledge of another's independent action does not produce vicarious responsibility absent some manifestation of consent or the ability to control," and it is only with active encouragement that this control is created.[56] By narrowly limiting the standard of acquiescence needed to produce a Fourth Amendment violation, courts are presumably concerned with limiting government liability in search and seizure cases. But in cases such as the one at issue, where a hacker is free to search a person's computer in hopes of finding incriminating information, does this standard provide sufficient Fourth Amendment protection?

As in *Jarrett*, significant Fourth Amendment issues arise once a hacker decides to turn over any incriminating information to law enforcement. The key inquiry here is whether an agency relationship existed between the hacker and law enforcement. As mentioned above, well-settled case law requires active encouragement on the part of the government to establish an agency relationship for search and seizure issues. But as one commentator puts it, "[w]hen the ability to search without burden increases, does the government's power to search increase as well?"[57] "Or, '[i]s freedom inversely related to the efficiency of the available means of surveillance? If so, we have much to fear.'"[58]

In the context of hacking, the requirement that a party exercise active acquiescence to establish an agency relationship does not afford adequate Fourth Amendment protection. The nature of a hacker's computer search is different than the nature of search methods typically addressed under relevant precedent.[59] The

54. Although both courts ultimately differed in their conclusion, the standard of acquiescence was the same.

55. *Jarrett*, 338 F.3d at 345 (quoting United States v. Koenig, 856 F.2d 843, 850 (7th Cir. 1988)).

56. *Id.*

57. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 18 (1999).

58. *Id.* (quoting JAMES BOYLE, SHAMANS, SOFTWARE, AND SPLEENS: LAW AND THE CONSTRUCTION OF THE INFORMATION SOCIETY 4 (1996)).

59. *See* Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. CAL. INTERDISC. L.J. 63, 85 (2001) (stating that unlike traditional crimes, hacking is prosecuted less because of several interrelated factors, including the problem of ano-

search is distinctive because it occurs in virtual space rather than in real space. This distinction is important for several reasons. First, a search in virtual space requires little skill and effort.[60] While hacking once required a large amount of computer expertise, today relatively little computer skill is needed to hack.[61] The modern recreational hacker can easily search various websites for "detailed instructions on hacking techniques and downloadable, do-it-yourself hacking tools."[62] As a matter of fact, Unknownuser ran across hacking software while looking for other programs on the Internet and stated that he found Dr. Steiger's information the first time he used the software.[63] In an email he wrote to law enforcement in the *Steiger* case, Unknownuser stated that he was not a "computer freak;" rather, he was a thirty-three-year-old professional who hacked for a hobby.[64] Additionally, because of the nature of cyberspace, hackers are able to search quickly and efficiently.[65] For instance, Unknownuser told FBI Agent Duffy about his ability to search thousands of computers with relative ease.[66] Most importantly, hackers have the ability to remain anonymous.[67] Thus, the government has trouble locating hackers and, as a consequence, cannot prosecute them. Moreover, foreign hackers are not subject to U.S. laws and the U.S. may not make a foreign country prose-

nymity, jurisdictional issues, and the lack of resources in the law enforcement community).

60. *See* Mary M. Calkins, Note, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 GEO. L.J. 171, 176 (2000) (stating that today's hackers come from many walks of life including juveniles with little computer knowledge who easily obtain effective hacking tools on the Internet).

61. *See id. See also* Eric J. Sinrod & William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177, 185 (2000) (stating that while hacking once required a fair amount of skill or computer knowledge, the recreational hacker today can now download attack scripts and protocols from the Internet and launch them against victim sites with little knowledge of the systems they are attacking).

62. Calkins, *supra* note 60, at 176.

63. *Jarrett*, 229 F. Supp. 2d at 514.

64. United States v. Steiger, 318 F.3d 1039, 1043 (11th Cir. 2003).

65. *See* Michael Edmund O'Neill, *Old Crimes in New Battles: Sanctioning Cyber Crimes*, 9 GEO. MASON L. REV. 237 (discussing the increased efficiency that computers provide to a criminal enterprise).

66. *Jarrett*, 229 F. Supp. 2d at 509.

67. Elizabeth Reiter, *The Department of Defense DNA Repository: Practical Analysis of the Government's Interest and the Potential for Genetic Discrimination*, 47 BUFF. L. REV. 975, 1018 (1999).

cute, especially if cyber-crime laws do not exist in that country.[68] As in *Jarrett*, this anonymity and invulnerability from prosecution creates an unintentional grant of immunity from prosecution.[69] This is dangerous because once a hacker commences a search of a personal computer, *all* information is available; whether it is incriminating or not.[70] So while hackers may be searching for incriminating evidence, they may also be searching for personal and financial information without fear of prosecution. Lastly, computer crimes often tend to be marginalized.[71] The reason for this may be that the injuries and stigmas associated with cyber-crimes are not seen as serious as the injuries, *mens rea*, and stigmas associated with crimes in real space.[72] This marginalization leads to a different perception and treatment of cyber-crimes. An act that would be blatantly unacceptable in real space may have its virtual counterpart become less objectionable because no significant injury is sustained. If the scenario changed to one where private individuals made it a habit to illegally search people's homes for incriminating evidence to subsequently hand over to law enforcement, then the public might demand a change in the law. However, this scenario is improbable. Searching homes requires significant effort, and as the number of homes searched increases, the likelier it is for a person to be caught.[73] Thus, the traditional agency requirement of active acquiescence is suitable in real space but problematic when applied to cyberspace.

68. Daniel M. Creekman, Note and Comment, *A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China*, 17 AM. U. INT'L L. REV. 641, 657-62 (2002).

69. This immunity puts the government in the position of implicitly encouraging a hacker's illegal behavior.

70. *See* Mark J. Maier, *Backdoor Liability from Internet Telecommuters*, 6 COMP. L. REV. & TECH. J. 27, 33 (2001) (explaining how hackers use "Trojan Horse" programs to gain complete access to a computer).

71. *See* Terri A. Cutrera, Note, *The Constitution in Cyberspace: The Fundamental Rights of Computer Users*, 60 UMKC L. REV. 139, 141 (1991) (explaining how law enforcement had for years marginalized computer crimes).

72. *See generally* Catherine Therese Clarke, *From Criminet to Cyber-Perp: Toward an Inclusive Approach to Policing the Evolving Criminal Mens Rea on the Internet*, 75 OR. L. REV. 191 (1996).

73. David A. Dana, *Rethinking the Puzzle of Escalating Penalties for Repeat Offenders*, 110 YALE L. J. 733, 750-53 (2001) (explaining that over the long run the probability increases for repeat offenders to be caught).

To afford adequate Fourth Amendment protection from hacking, the two-part test for an agency relationship in Internet search and seizure cases should replace the active acquiescence element with passive acquiescence.[74] With a passive acquiescence requirement, the court's two-part test for an agency relationship would consist of the following two inquiries: (1) whether the individual acted with motives to help law enforcement[75]; and (2) whether the government knew of and passively acquiesced in the search. Part two of the test is satisfied if the government has knowledge that an individual provided the government with information by hacking on prior occasions and the government has used the information in a criminal investigation.[76] In *Jarrett* then, for example, the acquiescence element of the agency test would be satisfied because the government knew that Unknownuser transmitted information obtained through hacking to the government on prior occasions and that he intended to continue the same type of activity. Such a strict test is the best way to give a person adequate protection from hackers turning over personal information to the government in violation of the Fourth Amendment.

While it may be argued that an active acquiescence standard is necessary because it allows the government to prosecute individuals who otherwise could not be prosecuted, Fourth Amendment rights should be of paramount concern. Some commentators have argued that use of private hackers may be necessary to compensate for law enforcement's inadequacies in technical sophistication and

74. This would not be the first time courts have interpreted acquiescence to be passive. In Zheng v. Ashcroft, 332 F.3d 1186, 1193 (9th Cir. 2003), the court, in interpreting 8 C.F.R. § 208.18(a)(7) (Implementation of the Convention Against Torture), defined acquiescence to require only "awareness" and not to require "actual knowledge" or "willful acceptance."

75. This part of the agency relationship test remains unchanged.

76. Such a test is in accord with the RESTATEMENT (SECOND) OF AGENCY § 43(2) (1958) (stating "acquiescence by the principal in a series of acts by the agent indicates authorization to perform similar acts in the future"). The comments shed further light on this section: "Approval of a single authorized act does not, of itself, justify an inference of authority to repeat it. On the other hand, if the agent performs a series of acts of a similar nature, the failure of the principal to object to them is an indication that he consents to the performance of similar acts in the future under similar conditions. These inferences can be rebutted, however, and it can be shown that the agent was not authorized." RESTATEMENT (SECOND) OF AGENCY § 43(2), cmt. b (1958).

experience.[77] However, this should not be an excuse to blatantly disregard a person's Fourth Amendment right against unreasonable searches and seizures. The current agency standard allows a private hacker to *continually* send incriminating information to the government for the purpose of prosecuting others so long as active solicitations are not made. As seen in *Jarrett*, the nature of cyberspace allows hackers to remain anonymous and avoid prosecution while continuing to illegally search computers. This enables the government to use illegally obtained incriminating information from the same hacker countless times in violation of the very essence of the Fourth Amendment.[78] A requirement of passive acquiescence would effectively curb the government from crossing the line into the realm of unconstitutionality in order to prosecute defendants that the government itself has trouble policing.

In *Jarrett*, the court essentially used an old law approach inadequately designed to deal with modern issues. In turn, the court produced a disquieting result. Hacking differs from traditional types of searches because it is anonymous, requires little skill and time, the tools are easily obtained, and the scope of the search is extensive. A person is entitled to a reasonable expectation of privacy in his or her computer files[79] and when technology allows private individuals to illegally search computers and establish relationships with law enforcement with almost no burden, judicial interpretations of agency and search and seizure laws must adapt. The court here has failed to do that. It is troubling to think that with this result, as long as no active solicitations are made, the government can establish relationships with known private hackers through suggestive thank you notes, and repeatedly accept information for purposes of prosecution. Moreover, because most hackers remain anonymous they obtain an unintentional immunity from the government for their activities and are unaccountable for their

77. *See* William R. Graham, Jr., Comment, *Uncovering and Eliminating Child Pornography Rings on the Internet: Issues Regarding and Avenues Facilitating Law Enforcement's Access to 'Wonderland',* 2000 L. REV. M.S.U.-D.C.L. 457 (2000).

78. The essence of the Fourth Amendment is to safeguard the privacy and security of individuals against arbitrary invasion by governmental officials by imposing a standard of reasonableness upon the exercise of those officials' discretion. U.S. CONST. amend. IV.

79. *See* Trulock v. Freehe, 275 F.3d 391 (4th Cir. 2001) (stating that a person is entitled to a reasonable expectation of privacy in password protected computer files).

actions. This provides no incentive to stop illegal behavior and, at the very least, promotes cyber-vigilantism. Unknownuser's actions would not be tolerated in real space and there is no reason why they should be allowed in cyberspace. Thus, in cases with facts similar to *Jarrett's*, courts should replace the active acquiescence element in the agency test with an element of passive acquiescence. It is only through this new strict standard that a person's Fourth Amendment rights can be adequately safeguarded.