EMOTIONAL ABROGATION: HOW INTERNET CHILD PORNOGRAPHY PROSECUTION IMPACTS SEARCH AND SEIZURE OF COMPUTERS IN OTHER CRIMES

KYRIAKI COUNCIL*

As computers become increasingly significant in our daily lives, and as other computer crimes begin to increase, courts have little else to rely on for computer search and seizure jurisprudence than the massive body of child pornography case law that has developed. Child pornography is the most frequently prosecuted computer crime. Though other computer crime cases are on the rise, courts often find themselves at a loss as to how to deal with the search and seizure of computers when they are used in a crime. Because there is little case law regarding computer crimes and few salient analogues for courts to use in their reasoning, computer crime case law must develop within a vacuum or void, or use the line of Fourth Amendment case law that has developed surrounding child pornography. This note analyzes child pornography prosecutions and the body of case law developed from those prosecutions, which allow the government to seize personal computers based upon arguably tenuous probable cause. This note further argues that there is a particular risk involved with analyzing computer crimes in a vacuum: that emotion, politics, or force may precede, or even supersede sound legal reasoning in the search and seizure of computers in other crimes.

* Kyriaki (Kiki) Council, B.A., University of Chicago, is a J.D. Candidate 2017 at the University of Colorado Law School. She will be clerking for the Honorable Justice Allison Eid on the Colorado Supreme Court after graduation, and will join the commercial litigation group at Holland & Hart in 2018. Kiki served as the Lead Student Note Editor for Volume 15 of the Colorado Technology Law Journal (CTLJ), and participated in CU Law's Technology Law & Policy Clinic. Kiki wishes to thank all those who supported her note writing journey, including: all members, past and present, of the CTLJ; Jordan Underhill & Calli Schroeder, for their endless editing and support; Professors Aya Gruber, Blake Reid, Ahmed White, Amy Griffin, Justin Desautels-Stein, for encouraging and supporting Kiki's love of academia, writing, and the law; her grandmother Kiki Brown, mother Irene Brown, and sister Lula Council, for their boundless love and ability to mitigate law-school induced panic; and finally her partner Jack Falk, for everything.

INTRODUCTION 436
I. SUBWAY AND SILK ROAD: CONTEMPORARY EXAMPLES OF COMPUTER CRIME SEARCH AND SEIZURE 438
II. A BRIEF HISTORY OF COMPUTER CRIME STATUTES 442
A. *Child Pornography Statutes* 442
B. *Investigation and Prosecution of Internet Child Pornography* 444
C. *Other Computer Crime Statutes* 445
D. *Investigation and Prosecution of Other Computer Crimes* 447
III. FOURTH AMENDMENT ABROGATION IN CHILD PORNOGRAPHY PROSECUTION 448
A. *United States v. Renigar: An Exploration of Probable Cause and Nexus* 448
B. *United States v. Burkhart: The Disappearance of Staleness* 450
IV. THE SPILLOVER EFFECT: AN EXPLORATION OF OTHER COMPUTER CRIME CASES 453
A. *United States v. Christie: The "How" vs. the "What" of Computer Search and Seizure in Light of Child Pornography Case Law* 453
B. *United States v. Ulbricht: Drug Dealers and Hidden Traps* 456
V. IS BALANCE POSSIBLE IN LIGHT OF CASES THAT EMOTIONALLY ABROGATE? 458
CONCLUSION 462

INTRODUCTION

In 2015, America was shocked to find that Subway spokesperson Jared Fogle was an accused child pornographer.[1] Only a few months before Fogle's home was raided, computers searched, and trove of child pornography discovered, Ross Ulbricht, creator of the online drug marketplace, Silk Road, was successfully prosecuted and convicted as a sex offender.[2] The search of the men's homes, computers, and personal effects will serve as the frame for this paper. This note explores the "emotional" spillover effect child pornography prosecutions in the Tenth Circuit have had on search and seizure determinations in

1. Hayley Peterson, *The Investigation into 'Subway Diet' Spokesman Jared Fogle Is Still a Mystery*, BUS. INSIDER (July 29, 2015, 8:30 AM), http://read.bi/1DaDIT1 [https://perma.cc/KZX6-7VUS].

2. Andy Greenberg, *Silk Road Mastermind Ross Ulbricht Convicted of All 7 Charges*, WIRED (Feb. 4, 2015, 3:57 PM), http://www.wired.com/2015/02/silk-road-ross-ulbricht-verdict/ [https://perma.cc/BDH6-5WYL].

other computer crimes.[3]

As computers become increasingly significant in our daily lives, and as other computer crimes begin to increase, courts have little else to rely on for computer search and seizure jurisprudence than the massive body of child pornography case law that has developed. As discussed below, child pornography prosecutions and the line of subsequent cases allow the government to seize personal computers based upon arguably tenuous probable cause. Further, this body of case law allows the government to search those personal computers with little limitation or particularity as to what can be searched on that computer. Once the government searches a computer nothing on the device will remain private. A search of a computer may justify the search of a home.

Because all that is needed to justify search and seizure of a computer is probable cause, every citizen is at potential risk for a governmental invasion of privacy. For the past 15 years, scholars have noted that child pornography prosecution abrogates the Fourth Amendment.[4] Child pornography is also the most widely litigated and prosecuted computer crime—so much so that one can hardly conduct legal research for "computer crimes" without stumbling upon hundreds of results all relating to child pornography.[5] Internet child pornography cases, though widely litigated, are not so specialized and well-developed as to insulate its abrogating effects from other computer crime cases, especially those involving emotional subjects like childhood neglect, or drug trafficking. Child pornography statutes and case law are inspired by sadness, anger, and fear. They demonstrate that courts and legislatures alike can abrogate the Fourth Amendment in any crime involving a computer. The danger of this abrogation becomes especially apparent when considering other computer crime statutes. This trend in Fourth Amendment computer search and seizure jurisprudence should be critically examined. Computer crime case law is beginning to develop more robustly,

3. "Emotional" means a criminal law subject that incites and invokes sadness, anger or fear in everyday citizens, as well as jurists. Crimes involving children (extremely vulnerable victims) tend to incite these emotions, leading society, legislators, and jurists alike to spring into action to prevent similar crimes in the future. Crimes like drug trafficking also invoke emotion. Many citizens, legislators, and jurists pin drug sale and its use as a criminal activity that destroys the fabric of society. As with child pornography, society seeks to end and prevent drug-oriented crime. There is nothing wrong with these goals, and I do not mean to argue as much.

4. *See, e.g.*, Anton L. Janik, Jr., *Combating the Illicit Internet: Decisions by the Tenth Circuit to Apply Harsher Sentences and Lessened Search Requirements to Child Pornographers Using Computers*, 79 DEN. U. L. REV. 379 (2002).

5. For example, searching for "computer crimes" in the Tenth Circuit generates 597 search results, the vast majority of which relate to child pornography. *See also FBI Claims 2,500 Percent Increase in Child Porn Arrests*, PRISON LEGAL NEWS (Oct. 2011), https://www.prisonlegalnews.org/news/2011/oct/15/fbi-claims-2500-percent-increase-in-child-porn-arrests/ [https://perma.cc/P527-6YX5].

and computers will continue to play an increasingly significant role in our daily lives. If courts do not tread lightly in this developing area of law, and continue to extend the emotional reasoning of child pornography case law, abrogation of the Fourth Amendment will spill over to every crime committed on a computer.

To explore these ideas, this note will proceed as follows: first, Part I frames the issue within two contemporary cases: the Jared Fogle child pornography investigation, search, seizure, and prosecution; and the Ross Ulbricht Silk Road investigation, search, seizure, and prosecution. These cases frame the general Fourth Amendment issues in computer crimes and the relationship (or lack thereof) between the reasoning and rhetoric used to prosecute these crimes. Part II will explore the history of child pornography statutes and cases, and delves into the various methods of investigating and prosecuting child pornography defendants. Part III identifies the issue of Fourth Amendment abrogation in child pornography cases by exploring two seminal Tenth Circuit cases. The section will also identify the reasoning that these child pornography cases employ for cutting Fourth Amendment protections short. Part IV then analyzes other computer crime cases that deal with Fourth Amendment search and seizure issues, and dissects the reasoning for denying the defendant Fourth Amendment protections. Part V explores the wider implications of the spillover effect of child pornography prosecution into other search and seizure cases involving computers. Exploration of these other computer crime cases reveal that Fourth Amendment-abrogative child pornography cases can be applied to the seizure and widespread, un-particularized search of a personal computer in any case involving emotional subject matter or vulnerable victims. This is especially true where the fear of defendants who are able to manipulate technology to shield their crimes is present.

I. SUBWAY AND SILK ROAD: CONTEMPORARY EXAMPLES OF COMPUTER CRIME SEARCH AND SEIZURE

On September 2014, a Jane Doe went to the Indiana State Police with text messages from Russell Taylor, the head of the Jared Foundation—the organization founded by Jared Fogle, of Subway fame.[6] Jane Doe told a state trooper that Taylor had offered to send her images or videos of young girls through text messages.[7] The alleged text messages included discussions of

6. Tim Evans & Mark Alesia, *Murky Profile of Ex-Jared Foundation Leader Emerges*, USA TODAY (July 12, 2015, 3:06 PM), http://usat.ly/1ITPGBc [https://perma.cc/S5KG-5W9U].

7. *Id.*

sexual matters, "including bestiality and sadistic or masochistic abuse."[8] An affidavit in support of a search warrant was filed the following April in federal court. The search warrant and Jane Doe's response were passed on to an IMPD Cybercrime Unit detective.

The investigation intensified following an interview with Jane Doe in early October 2014. Doe told investigators she did not delete the incriminating messages from Taylor and gave investigators access to her cellular phone. The text message from Taylor concerned Doe conducting an act of bestiality with another woman.[9] An image file accompanied the text from Taylor; it depicted an act of bestiality. Doe did not retain any text messages from Taylor asking her if she wanted to view images of young girls, but she said they were sent. Doe claimed Taylor traveled to Thailand in the past.[10] The affidavit for search warrant noted, "[s]ome persons who have sexual interest in children have been known to travel to Thailand to engage in child sex tourism."[11]

The original purpose of the search warrant was to look for evidence of bestiality, including images or videos. Police did not uncover these types of videos and images during the search, but they did discover a "shocking" amount of child pornography.[12] The items seized included a thumb drive that contained "videos of child pornography and child erotic" and "documents related to [Taylor's] employment as director of a foundation [the Jared Foundation]."[13]

Less than two months later, authorities raided Jared Fogle's home. Law enforcement authorities spent eleven hours removing computers, documents, and other items. It is still unclear what led authorities to Jared Fogle's home—whether it was the hard drive that contained child pornography and the document from the Jared Foundation, or something else such as surveillance or recovery of emails between Fogle and Taylor. It is clear that one woman's text message led to the recovery of a shocking trove of child pornography via affidavits for another sexual crime.

Fogle's case is not rare among child pornography investigations and prosecutions. Many child pornographers are caught and charged in a similar manner: someone—a law enforcement agency, family member, or friend—discovers the

8. *Id.*
9. *Id.*
10. *Id.*
11. Thailand is known as a haven for child pornography and child sex tourism. *See Strengthening Thai Laws to Fight Travellers Who Sexually Abuse Children*, U. N. OFFICE ON DRUGS & CRIME (Mar. 14, 2012), http://www.unodc.org/southeastasiaandpacific/en/2012/03/childhood-workshop-thailand/story.html [https://perma.cc/3KB6-NL69].
12. Evans & Alesia, *supra* note 6.
13. *Id.*

defendant's child pornography collection or hears of it, an investigation is launched, and after a period of surveillance, a search warrant is issued accompanied by an affidavit. This search warrant may reach the defendant's computer and whatever images or files are within it. The reverse is also true: Internet surveillance of child pornography related activity can lead to a widespread and far-reaching search of a defendant's home.[14]

Child pornography is not the only prosecuted computer crime. As the Internet and related technologies grow, so does the potential for various other computer crimes including identity theft, accessing a computer and obtaining information, intentionally damaging by knowing transmission, trafficking in passwords, extortion involving computers, disclosing an intercepted communication, unlawful access to stored communications, and even disseminating misleading spam.[15] Other "everyday" or "real life" crimes can also be committed on computers including prostitution, drug sales, attempt or conspiracy to attempt murder, or money laundering.[16]

The prosecution of Ross Ulbricht—the so-called "evil mastermind" behind Silk Road—is a prime example of one of these other computer crimes.[17] Silk Road was an illicit online marketplace used for the sale of drugs, fake IDs, weapons, and other illegal items. Users could only access the marketplace on the Deep Web—a portion of the Internet not indexed by search engines, and therefore hidden from the view of the general Internet-using public.[18] Sometimes these websites are encrypted and require programs to gain access. These portions of the Internet are called the Dark Net. The software needed to gain access to these sites also makes the user anonymous, meaning their Internet protocol (IP) addresses and other identifying information are not logged when they access the website.[19]

The illicit nature of the Silk Road caught the attention of law enforcement. Ross Ulbricht, the creator of the forum, was tracked down via a sting operation that investigated Ulbricht and Silk

14. *See, e.g.*, United States v. Veater, 576 F. App'x 846 (10th Cir. 2014).

15. *See generally* OFFICE OF LEGAL EDUC. EXEC. OFFICE FOR U.S. ATT'YS, PROSECUTING COMPUTER CRIMES (2015) (describing how to prosecute computer crimes under current law including remedies) [hereinafter PROSECUTING COMPUTER CRIMES].

16. *See, e.g.*, United States v. Burgess, 576 F.3d 1078 (10th Cir. 2009) (finding a search limited to evidence of drug trafficking information likely to be found on a computer, such as a pay-owe sheet and address books, to be valid).

17. Jessica Roy, *What Exactly is Going on with the Silk Road Case?*, N.Y. MAG. (Jan. 16, 2015, 2:53 PM), http://nymag.com/daily/intelligencer/2014/11/explainer-why-the-fbi-shut-down-dark-net-sites.html [https://perma.cc/J8CG-VTPM].

18. *See* Jose Pagliery, *The Deep Web You Don't Know About*, CNN TECH (Mar. 10, 2014, 9:18 AM), http://cnnmon.ie/1lo8avw [https://perma.cc/AVK5-B528] (explaining further about the deep web).

19. *Id.*

Road over the course of two years.[20] This investigation stretched internationally because Iceland housed the server hosting Silk Road. In July 2013, the government conducted "imaging" of the server.[21] Information from the Icelandic server led to orders for "pen-registers and trap and trace devices," as well as "warrants to seize and then search a number of other servers located within the United States."[22] The warrants also requested the search and seizure of a laptop associated with Ulbricht, his Facebook account, and his Gmail account. The government obtained a total of fourteen warrants and court orders over the course of the investigation.

The various warrants, seizures, and searches led investigators to Ulbricht in San Francisco. Agents set up a sting and observed Ulbricht using his laptop computer. During the investigation, an undercover agent using several Silk Road accounts developed a relationship with "Dread Pirate Roberts"—Ulbricht's pseudonym.[23] The undercover agent became an administrator, and started a conversation with Dread Pirate Roberts, requiring Ulbricht to open an "administrator panel" on his Internet browser. This was done while FBI agents watched Ulbricht. When Ulbricht logged in as an administrator the federal agents seized him and his laptop.

The subsequent searches of Ulbricht's personal computer revealed a journal and logbook that detailed his activities running Silk Road. The U.S. Attorney for the Southern District of New York charged Ulbricht with several crimes including narcotics conspiracy, conspiracy to commit computer hacking, money laundering, and several attempted murder conspiracies.[24]

Ulbricht's attorneys attempted to suppress all evidence that stemmed from the search and seizure of the Icelandic server. They argued that the search and seizure, in addition to the search and seizure of servers in Pennsylvania and of Ulbricht's laptop, Facebook, and Gmail accounts, were unconstitutionally general.[25] These arguments relied primarily upon his privacy interests within these items—including the servers themselves. However, Ulbricht never conceded that he committed these crimes, merely

20. Jessica Roy, *Feds Raid Online Drug Market Silk Road*, TIME (Oct. 2, 2013), http://ti.me/19YRCDZ [https://perma.cc/BH6R-3RCU].

21. "Imaging" of a server means creation of an image file that can include the system's data, operating system, programs, software updates, patches, mission critical data files, configurations, settings, and e-mails. *See Server Imaging*, 4SERVICES INC., http://www.4service.com/server_imaging.asp. [https://perma.cc/EP9B-AXRC] (last visited Mar. 22, 2016).

22. United States v. Ulbricht, No. 14-CR-68 KBF, 2014 WL 5090039, at *2 (S.D.N.Y. Oct. 10, 2014).

23. Roy, *supra* note 19.

24. United States v. Ulbricht, 31 F. Supp. 3d 540, 546 (S.D.N.Y. 2014).

25. Ulbricht, s*upra* note 23, at *3.

that his interest in these things were "manifest."[26] The district court judge disagreed (analyzed below) and denied the motions to suppress. Ulbricht was convicted of all charges and sentenced to life imprisonment.

Investigations like those of Fogle and Ulbricht reveal the real danger computer crimes pose to U.S. individual's Fourth Amendment rights. While their crimes may seem complicated and too advanced or far-fetched for any ordinary[27] citizen to commit, the Fogle and Ulbricht cases demonstrate how the search and seizure of computers can have far-reaching and long lasting effects for all citizens.

II. A BRIEF HISTORY OF COMPUTER CRIME STATUTES

A. CHILD PORNOGRAPHY STATUTES

To better understand the magnitude of child pornography search and seizure and how the jurisprudence may affect other computer crimes, it is necessary to understand the background of Internet child pornography litigation and prosecution in the United States.

Child pornography is a growing issue in the United States and throughout the world. In 2007, there were an estimated fourteen million child pornography websites that posted several thousand images each week. Reports of child pornography to the National Center for Missing and Exploited Children's CyberTip-line increased from around 3,000 reports in 1998 to over 100,000 in 2004.[28]

Laws prohibiting child pornography did not materialize until the 1970s, starting with the state of New York. In 1984, Congress passed the Child Protection Act, which removed almost all First Amendment protections from the category of child pornography by automatically deeming any representation of sex with a minor as obscene and illegal.[29] Three bills followed the Child Protection Act: the U.S. Child Sexual Abuse and Pornography Act, the Child Protection and Obscenity Enforcement Act, and finally the Child Protection Restoration and Penalties Enforcement Act.[30] This triad of statutes focused primarily upon the advertising of child pornography; the use of computers for the dissemination of child

26. Ulbricht, s*upra* note 23, at *1.

27. "Ordinary" refers to citizens who are not multi-million celebrities like Fogle or citizens who are not extremely technologically sophisticated, like Ulbricht.

28. Michael J. Henzey, *Going on the Offensive: A Comprehensive Overview of Internet Child Pornography Distribution and Aggressive Legal Action*, 11 APPALACHIAN J.L. 1, 2 (2011).

29. Child Protection Act of 1984, 18 U.S.C. § 2251 (2012).

30. Henzey, *supra* note 27, at 14.

pornography; record-keeping requirements for the producers of legal, adult sexually explicit materials; and criminalization of the possession of child pornography. The acts virtually eliminated child pornography in the United States. However, it resurged with the advent of the Internet.[31]

In the 1990s, federal child pornography statutes focused more on the Internet and its potential exploitation by criminals.[32] Three acts were passed: the Child Pornography Prevention Act (CPPA), the Protection of Children from Sexual Predators Act, and the Children's Online Privacy Protection Act. Of these, the CPPA is the most significant.[33] CPPA redefined child pornography federally and outlawed pornographic images that did not utilize actual children in its production.[34]

Congress and subsequent executive administrations have continued to focus on child pornography criminalization and prosecution around preventing the exploitation of children. These efforts are exemplified by the Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act of 2003 (the "PROTECT Act").[35] The PROTECT Act aimed to criminalize non-obscene virtual child pornography in a way that passed constitutional muster.

Of particular relevance to this note, 18 U.S.C. § 2258(A) is a provision that imposes certain reporting requirements of child pornography for electronic service providers. Under the statute:

> [W]hoever, while engaged in providing an electronic communication service or a report computing service to the public through a facility or means of interstate or foreign commerce, obtains actual knowledge of any facts or circumstances described in [relevant federal child pornography prosecution statutes] shall, as soon as reasonably possible make a report to the CyberTipLine of the National Center for Missing and Exploited Children (NCMEC).[36]

NCMEC[37] must forward this information to the appropriate

31. Henzey, *supra* note 27, at 1.

32. Henzey, *supra* note 27, at 5.

33. Henzey, *supra* note 27, at 18.

34. *See* 18 U.S.C. § 2252 (2012); *Id.* § 2252(A); Child Protection Act of 2012, Pub. L. No. 112-206, 126 Stat 1490-94 (2012).

35. Prosecutorial Remedies and Tools Against the Exploitation of Children Today Act of 2003 (PROTECT Act), Pub. L. No. 108-21, 117 Stat 650-95 (2003).

36. 18 U.S.C. § 2258A(a)(1) (2012).

37. NCMEC is a non-profit organization founded in 1984 by John and Reve Walsh after their son Adam disappeared. The organization was created in an effort to aid law enforcements like the FBI in locating missing children and to prevent child victimization. Prior to 1984, there was no centralized crime database for missing or stolen children. NCMEC created the CypberTipline in 1998, which is now the national

law enforcement agency after this report is made. The penalties for failing to report are significant. Willful failure to report child pornography websites or activities can incur an Internet service provider (ISP) a fine of $150,000. A second willful failure can result in a $300,000 fine.[38] The statute specifically provides for the fact that ISPs may not themselves conduct special surveillance. Instead, the statute focuses the responsibility of ISPs to mandated reporting.[39]

B. INVESTIGATION AND PROSECUTION OF INTERNET CHILD PORNOGRAPHY

Child pornography, like other computer crimes, is discovered (or uncovered) in many ways. Some agencies conduct undercover sting operations on pedophile and child pornography related Internet forums to collect evidence, while others set up "honey trap sites"—where phony child pornography sites are established to capture the details of offenders who attempt to access the supposed pornography.[40] Other agencies publicize crackdowns or conducting traditional criminal investigations.[41]

Another method is "RoundUp"—a government surveillance program that contains image caches of child pornography collected by the government over the course of several years.[42] The government runs the RoundUp image surveillance, looking for computers accessing the cached images before capturing IP addresses of those computers within the system. The government then compels the responsible ISP to disclose the name and address of the owner of the IP address. Reports may also come from friends, family members and even computer repair shops. Moreover, some law enforcement agencies receive reports from the NCMEC.

After incriminating facts have been compiled, agencies file for a search warrant, attach an accompanying affidavit describing the nature of the alleged crime, and provide reasoning for the warrant

---

mechanism for the public and electronic service providers to report suspected child exploitation. NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN, http://www.missingkids.org/History [https://perma.cc/VLX7-PVA2] (last visited Apr. 11, 2016).

38. *Id.* §§ 2258A(e)(1)–(2).

39. *Id.*

40. Richard Wortley & Stephen Smallbone, *Child Pornography on the Internet: The Problem of Internet Child Pornography*, CTR. PROBLEM-ORIENTED POLICING, http://www.popcenter.org/problems/child_pornography/print/ [https://perma.cc/S87K-7DGP] (last visited Feb. 19, 2017).

41. *Id.* at 22 n.85.

42. Janis Wolak et al., *Measuring A Year of Child Pornography Trafficking by U.S. Computers on a Peer-to-Peer Network*, 38 CHILD ABUSE & NEGLECT 347 (2013).

itself.[43] As stated earlier, this search warrant can reach as far into the home of the child pornographer as the government finds necessary. If "hard copy" child pornography is discovered in a home (or reported by a friend or family member) then the subsequently issued search warrant may reach to computers as well—with slight justification needed for doing so.[44] This was the case with both Jared Fogle and Russell Taylor.

The search of the computer itself can be vast; many jurisdictions have argued that there need not be any sort of particularity within the warrant itself. In other words, a law enforcement agency need not limit its request to search a portion of a computer, such as a specific file, hard drive, or flash drive. A request to search for an "image file" within a certain location is often a sufficient justification to search the entire computer. This conduct is justified by, the presumption that criminals often attempt to hide their illicit behavior.[45] In some cases, however, defendants are able to successfully argue that decrypting portions of hidden hard drives violates their Fifth Amendment rights.[46] Search warrants for child pornography are also deemed by certain jurisdictions to retain their probable cause, even after several months or years.

C. OTHER COMPUTER CRIME STATUTES

How are other computer crimes investigated and prosecuted in comparison to child pornography? Computer crime statutes were derived in the 1980s,[47] although some existing acts, such as the Wiretap Act,[48] have been historically used (and amended) to prosecute certain "electronic communications."[49] The Department of Justice recommends using the Wiretap Act to prosecute computer crimes "whenever a case involves spyware users and manufacturers, intruders using packet sniffers, persons improperly cloning email accounts, or any other surreptitious

43. Affidavits of this sort are typical in criminal cases that require a search and seizure warrant.

44. *See, e.g.*, United States v. Riccardi, 405 F.3d 852, 860–61 (10th Cir. 2005) (affirming a finding of probable cause to search a computer where the affidavit alleged that the defendant called teenage boys for sexual gratification, his home contained hard-copy photos of child pornography, a receipt showed that he had digitized photographs, and in the investigating officer's experience, "possessors of child pornography often obtain and retain images of child pornography on their computers").

45. *See generally* United States v. Burkhart, 602 F.3d 1202, 1207 (10th Cir. 2010) (noting that the Tenth Circuit "repeatedly endorsed 'the view that possessors of child pornography are likely to hoard their materials and maintain them for significant periods of time.)

46. *See In re* Grand Jury Supoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012).

47. PROSECUTING COMPUTER CRIMES, *supra* note 15, at 1.

48. 18 U.S.C. § 2511(1) (2012).

49. PROSECUTING COMPUTER CRIMES, *supra* note 15, at 59.

collection of communications from a victims computers."[50]

Although the Wiretap Act was a viable statute for prosecution purposes, law enforcement agencies became increasingly concerned about how the wire and mail fraud statutes would combat new crimes emerging in the computer age. Thus, in the Comprehensive Crime Control Act of 1984, Congress included provisions to address "the unauthorized access and use of computers and computer networks."[51] Instead of adding provisions regarding computer crimes to existing criminal laws, federal computer-related offenses were addressed in a single, new statute.[52]

Over the next several months, Congress continued to hold hearings concerning potential computer crime bills. These hearings resulted in the Computer Fraud and Abuse Act (CFAA), enacted in 1986.[53] CFAA amended 18 U.S.C. § 1030. Within CFAA, several crimes with a "compelling federal interest" are proscribed, as well as other computer crimes including the theft of property via computer that occurs as a part of a scheme to defraud. Additionally, the CFAA contains provisions that penalize "those who intentionally alter, damage, or destroy data belonging to others."[54]

In addition to the CFAA and the Wiretap Act, several other statutes deal with crimes specifically committed using computers, such as Unlawful Access to Stored Communications,[55] identity theft,[56] access device fraud,[57] the CAN-SPAM Act of 2003,[58] wire fraud,[59] and communication interference.[60] Although federal statutes concerning computer crimes were originally borne to protect government and federal interests in interstate commerce, computer crime statutes have expanded in light of technological advancement, leaving the limitations of venue and jurisdiction behind.

---

50. PROSECUTING COMPUTER CRIMES, *supra* note 15, at 59.

51. PROSECUTING COMPUTER CRIMES, *supra* note 15, at 1.

[52] 18 U.S.C. § 1030

53. 18 U.S.C. § 1030 (2012).

54. PROSECUTING COMPUTER CRIMES, *supra* note 15, at 2.

55. 18 U.S.C. § 2701 (2012) (criminalizing intentional access to a facility, without authorization, through which an electronic communication service is provided, or intentionally exceed an authorization to access that facility).

56. 18 U.S.C. § 1028(a)(7) (2012) (criminalizing identity fraud).

57. 18 U.S.C. § 1029 (2012) (criminalizing credit card fraud).

58. 18 U.S.C. § 1037 (2012) (criminalizing email fraud, among other email related crimes).

59. 18 U.S.C. § 1343 (2012) (criminalizing fraud by wire, radio, or television).

60. 18 U.S.C. § 1362 (2012) (criminalizing abuse, fraud, or interference with communication lines, stations, or systems).

D. INVESTIGATION AND PROSECUTION OF OTHER COMPUTER CRIMES

As with child pornography investigations, computer crimes are often uncovered and prosecuted because of "real-time" electronic surveillance. Two statutes govern surveillance: the Wiretap Act, 18 U.S.C. §§ 2510-2522 (mentioned above), and the Pen/Trap statute, 18 U.S.C. §§ 3121-3127. Both statutory schemes regulate how a governmental agency can access different types of information. The Wiretap Act allows the government to obtain the contents of wire and electronic communications in transmission. The Pen/Trap statute allows the government to conduct a real-time collection of "addressing and other non-content information relating to those communications."[61]

As a simplified example, consider email. All emails consist of a set of "headers" containing address and route information generated by the email program, as well as the actual contents of the message authored by the email sender. The header includes the email of both the sender and recipient, and information about when and where the information was sent. The Pen/Trap statute allows law enforcement to collect the header information of an email by court order. The interception of the actual contents of the email, however, is governed by the Wiretap Act.

Under the Pen/Trap statute, an attorney may apply for a court order that approves the installation of a pen register, trap, or trace device "if the information likely to be obtained is relevant to an ongoing investigation."[62] The application must contain the identity of the applications, the identity of the law enforcement agency conducting the investigation, and a certification of the agency's belief that the information is relevant to the ongoing criminal investigation. The court issuing the order must also have valid jurisdiction. If the application has these elements, "the statute obligates the court to authorize the installation and use of a pen/trap device anywhere in the United States."[63] Perhaps alarming to some, "the court will not conduct an independent judicial inquiry into the veracity of the attested facts."[64] The statute does not require the agency seeking access to describe what types of "dialing, routing, addressing signaling information" it intends to collect.[65]

Under the amended Wiretap Act, electronic communication is

61. PROSECUTING COMPUTER CRIMES, *supra* note 15, at 152.

62. 18 U.S.C. § 3122(b)(2) (2012).

63. *Id. §* 3122(a); 18 U.S.C. § 3127 (2)(A) (2012); PROSECUTING COMPUTER CRIMES, *supra* note 15, at 155.

64. *See In re* Application of United States of America for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 846 F.Supp 1555, 1559 (M.D. Fla. 1994).

65. 18 U.S.C. § 3127(3) (2012).

a broad and catchall category. According to the Act's legislative history, "a communication is an electronic communication if it is neither carried by sound waves nor can be characterized as one containing the human voice (carried in part by wire)."[66] Most courts have held that to "intercept" this electronic communication under the statute, the communication must be acquired at the time of transmission. Accessing a stored copy of the communication is not to "intercept" the communication. Generally, the Wiretap Act prevents all third parties, including the government, from wiretapping phones, or installing "sniffers" to read Internet traffic.[67] There are, however, several exceptions.

Exceptions to the Wiretap Act include: interception pursuant to a court order, content exceptions, the provider exception, the computer trespasser exception, the extension telephone exception, the inadvertently obtained criminal evidence exception, and the accessible to the public exception.[68] The two most frequently used exceptions are those found in §§ 2511(2)(c) and (d). The first exception allows those "acting under color of law" to intercept electronic communications.[69] Whether one is acting under color of law is determined by whether the government actor was acting under the government's directions while conducting the interception. The second exception is broader. It states that those acting under color of law may lawfully intercept an electronic communication if they are party to the conversation, or where one of the parties "has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution."[70] In other words, the exception allows undercover agents communicating with potential criminals online to consent to a monitoring of that conversation. Understandably, these exceptions are used to investigate computer crimes, conduct sweeping surveillance of those who commit those crimes, and to prosecute crimes.

III. FOURTH AMENDMENT ABROGATION IN CHILD PORNOGRAPHY PROSECUTION

A. UNITED STATES V. RENIGAR: AN EXPLORATION OF PROBABLE CAUSE AND NEXUS

U.S. v. Renigar is a child pornography case concerning a

66. H.R. REP. No. 99-647, at 35 (1986).

67. PROSECUTING COMPUTER CRIMES, *supra* note 15, at 59.

68. *See* 18 U.S.C. § 2518 (2012); 18 U.S.C. § 2511(2)(a)(i), (2)(c)–(d), (2)(g)(i), (3)(b)(iv) (2012); 18 U.S.C. § 2510(5)(a) (2012).

69. 18 U.S.C. § 2511(2)(c).

70. *Id.* § 2511(2)(d).

search warrant affidavit and probable cause.[71] In *Renigar*, the defendant argued that the affidavit underlying the search warrant did not provide probable cause to search his residence. "Specifically, he argue[d] that tracing child pornography to an IP address which is associated with his residential address did not provide an adequate nexus between the evidence of the crimes alleged and the location to be searched."[72] *Renigar* provides an informative illustration of how a child pornographer is typically monitored and captured by the government. The affidavit for a search warrant of the defendant's effects contained the following information. The defendant was using a publicly available peer-to-peer (P2P) file-sharing network.[73] The assigned FBI agent connected a computer to another with a username associated with the defendant. That username made several files on his computer that contained child pornography available for download by other users on the P2P network, but the FBI agent was unable to download the files. A few months later, another FBI agent, in another state, accessed the same P2P network and successfully downloaded several of the files available on the computer. The defendant's IP address was discovered to be the same in both instances.[74]

With the defendant's IP address in hand, the FBI sought to obtain further information, leading the agents to the American Registry for Internet Numbers. The IP address in question was registered to Cox Communications ("Cox"). In accordance with federal statutes, Cox disclosed the name and address that the IP address was assigned to.[75] Other public record searches performed by the FBI positively identified the defendant as a resident of the address that was provided by the ISP. The details of the investigation—conducted by the FBI in the affidavit—included a section called "Background on Computers and Child Pornography."[76] The section described the process through which an individual may use a computer to access, store, and/or share computer files including child pornography. Additionally, it stated that even if a person intends to erase all evidence of the receipt, possession, and/or transmission of certain computer files, a record

71. United States v. Renigar, 613 F.3d 990 (10th Cir 2010).

72. *Id.* at 991.

73. "In its simplest form, a peer-to-peer (P2P) is created when two or more PCs are connected and share resources without going through a separate server computer. A P2P network can be an ad hoc connection – a couple of computers connected via a Universal Serial Bus to transfer files." James Cope, *How-to: Peer-to-Peer Network*, COMPUTERWORLD (Apr. 8, 2002, 1:00 AM), http://www.computerworld.com/article/2588287/networking/peer-to-peer-network.html [https://perma.cc/YD7F-64EB].

74. *Renigar*, 613 F.3d at 991.

75. *Id.* at 992.

76. *Id.* at 993.

of the activities may be preserved on a hard drive.[77]

The FBI executed the warrant, and the defendant was arrested. Agents seized a computer and several DVDs from the defendant's apartment. Each item contained child pornography. The defendant was indicted by a grand jury and charged under 18 U.S.C. §§ 2252(a)(4)(b) and (b)(2), as well as 18 U.S.C. §§ 2252(a)(2) and (b)(1). The defendant filed a motion to suppress the physical evidence by arguing that the affidavit failed to provide probable cause for the warrant, thereby causing his entire encounter with the FBI to be in violation of the Fourth Amendment. After the motion was denied, he entered a conditional guilty plea.

In *Renigar*, the court determined the FBI's affidavit furnished probable cause and that a nexus was adequately established between the evidence of the crime and the location to be searched.[78] In reviewing probable cause, appellate courts offer great deference to the issuing judge's finding. The only inquiry on appeal is to whether, under the totality of the circumstances presented in the affidavit, the judge had a substantial basis for determining that probable cause existed.[79] The court stated that "[t]he test is whether the facts presented in the affidavit would warrant a person of reasonable caution to believe that evidence of a crime will be found at the place to be searched."[80]

The *Renigar* court determined that because the IP address was linked to both child pornography and the physical address, and because of the affidavit's discussion of computer technology, the FBI had established a strong inference that the computer would be found at the apartment and would contain evidence associated with that child pornography and/or its transmission. It is important to note that the supplemental information regarding technology, not just the evidence related to the investigation itself, played a significant role in the court's determination as to whether the affidavit contained probable cause.

B. UNITED STATES V. BURKHART: THE DISAPPEARANCE OF STALENESS

U.S. v. Burkhart presents another probable cause search warrant case. In *Burkhart*, however, the defendant argued that probable cause did not support the search warrant because the warrant was executed two years after an email exchange with a porn distributor.[81] This specific case spread across international

77. *Id.*
78. *Id.* at 994.
79. *Id.*
80. *Id.*
81. United States v. Burkhart, 602 F.3d 1202 (10th Cir. 2010).

borders. In 2006, The European Law Enforcement Organization (Europol) investigated a child pornography ring. During the investigation, Europol came across an Italian citizen operating a child pornography website. The Italian's home was searched, and law enforcement uncovered thousands of incriminating emails. Europol sent the FBI several thousand emails between the Italian defendant and addresses located in the U.S. The FBI uncovered forty-five emails between the Italian and the defendant. The most recent email was dated to 2005 and verified purchases of videos of a 13-year-old girl.[82]

In April 2007, the FBI obtained an administrative subpoena for the email address owner's subscriber information. The FBI received the subpoena for AT&T, who confirmed the alleged name and address of the defendant. The defendant no longer lived at this residence. However, through DMV records, the FBI discovered that two vehicles were registered to the defendant at two different addresses in the same city and state.[83] The FBI prepared a search warrant for each of the addresses uncovered. Within the search warrant, the FBI agent set out:

> Agent Fitzer's training and experience in law enforcement generally, and computer storage systems and child pornography investigations in particular. The affidavits related how the Europol investigation led to a William David Burkhart, the nature of the videos believed to be in Mr. Burkhart's possession, the characteristics of child pornography collectors, and descriptions of the places to be searched and the items to be seized.[84]

The affidavit stated that certain cars registered to the defendant were located at the addresses, and that a mailbox at one of the residences had the defendant's last name on it. A magistrate judge reviewed the applications and affidavits in May 2008, and the warrant was executed two days later. At the second address, the agents found the defendant and several hundred DVDs with images of child pornography. The defendant moved to suppress the evidence uncovered at his home. After the district court denied the defendant's motion to suppress, he entered a conditional guilty plea of 18 U.S.C. § 2252(a)(4)(B) and was sentenced to 84 months of prison.[85]

The defendant argued that the FBI's affidavit did not establish probable cause to search his home for three reasons. First, by the time the FBI executed the warrants, the information

82. *Id.* at 1204.
83. *Id.* at 1204–05.
84. *Id.* at 1205.
85. *Id.*

from Europol was stale[86]; second, the affidavit failed to show a nexus between the suspected possession of child pornography and Mr. Burkhart's home; and third, each affidavit undermined the probable cause in the other affidavit.[87] In general, probable cause cannot be based on stale information, but staleness depends upon the nature of the crime, the length of the activity, and the nature of the property to be seized.[88] Though this search warrant was executed two years and four months after the last email, and though the defendant no longer lived at the mailing address provided to his email service provider, the court determined staleness did not apply.[89]

The court reasoned that the relevant factors are the "nature of the criminal activity and the nature of the property to be seized".[90] The age of the emails was held irrelevant because the defendant was charged with possession of child pornography, not acquisition of child pornography. The emails supported the court's finding that the defendant bought the videos because "one could reasonably infer that he likely still possessed the videos."[91] The court also determined the amount of enthusiastic emails exchanged with the pornography distributor played a role in determining guilt. The court cited the FBI agent's affidavit, which observed, "[c]ollectors typically retain [the materials] for many years."[92] Further, the Tenth Circuit "repeatedly endorsed 'the view that possessors of child pornography are likely to hoard their materials and maintain them for significant periods of time.'"[93] Courts cite this reasoning in child pornography prosecution appeals time and time again:[94]

> The reasoning is supported by common sense[95] and the cases. Since the materials are illegal to distribute and possess, initial collection is difficult. Having succeeded in obtaining images, collectors are unlikely to destroy them.

86. When executing a search warrant, the government must have probable cause. However, the government is limited in that the probable cause to search a house, or items, cannot be based on old or "stale" information that no longer suggests that the items sought will be found in the place to be searched. United States v. Mathis, 357 F.3d 1200, 1205 (10th Cir. 2004).

87. *Id.* at 1206.

88. *Burkhart*, 602 F.3d at 1202 (citing United States v. Mathis, 357 F.3d 1200, 1206-07 (10th Cir. 2004)).

89. *Id.* at 1207.

90. *Id.*

91. *Id.* at 1206.

92. *Id.*

93. *Id.*

94. *See* United States v. Potts, 586 F.3d 823, 830 (10th Cir. 2009); United States v. Perrine, 518 F.3d 1196, 1206 (10th Cir. 2008).

95. I am unsure what "common sense" means here. Was the defendant especially sophisticated in computer technology? Is he presumed to be a child pornographer after the fact?

> Because of the illegality and the imprimatur of severe social stigma such images carry, collectors will want to secret them in secure places like a private residence.[96]

The court notes that most cases supporting this proposition concerned regular mail, rather than "anonymous collection through the Internet."[97] The Internet works anonymously, enables easy use of credit cards for purchases, and lowers many of the practical barriers for any "collector" of child pornography. Due to these characteristics, the court found that the Internet context "may mitigate *against* staleness."[98] It followed that, "[i]nformation that a person received electronic images of child pornography is less likely than information about drugs, for example, to go stale because the electronic images are not subject to spoilage or consumption."[99] Unlike evidence of other crimes, electronic files "can have an infinite life span." Herein lies the dilemma: Internet crimes can never go away. Evidence of a crime is continually ongoing within the child pornography world because those who possess child pornography have been found by several courts to be "hoarders" or "collectors."

The court foreclosed the defendant's second argument about a nexus between the suspected criminal activity and the place to be searched. The nexus of the affidavit was found to be sound even though the incriminating email was more than two years old, the facts that the address registered to that email was no longer registered to the defendant, and two additional unconfirmed addresses were associated with the defendant. The court reasoned that the DMV registrations and the post office information, as well as a car matching the make and model of the defendant's car, sufficiently linked the defendant to the home and justified a search of its entirety.[100]

IV. THE SPILLOVER EFFECT: AN EXPLORATION OF OTHER COMPUTER CRIME CASES

A. UNITED STATES V. CHRISTIE: THE "HOW" VS. THE "WHAT" OF COMPUTER SEARCH AND SEIZURE IN LIGHT OF CHILD PORNOGRAPHY CASE LAW

The court in *U.S. v. Christie*[101] faced unsettling facts. The

96. United States v. Riccardi, 405 F.3d 852, 860–61 (10th Cir. 2005).

97. Burkhart, 602 F.3d at 1207 (quoting United States v. Lamb, 945 F.Supp 441, 460 (N.D.N.Y. 1996)).

98. *Id.* (emphasis added).

99. *Id.* (quoting United States v. Frechette, 583 F.3d 374, 378 (6th Cir. 2009).

100. *Id.*

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

defendant Rebecca Christie was charged with child abuse and the second-degree murder of her three-year-old child. Christie was presumably an Internet and/or gaming addict.[102] She often left her daughter in her bedroom, without food, water, or any semblance of the care. Christie's husband was deployed across the country. Within nine days of his departure, her child died due to malnutrition and dehydration. Much of the evidence presented against the defendant at trial came from the computer "she so prized."[103] The searches of this computer were the basis for Christie's appeal.

A court issued two search warrants for the computer. The first was issued five months after authorities seized the computer. Christie argued that this delay was constitutionally impermissible.[104] Despite concerns regarding the delay, the Circuit Court upheld the first search warrant. The second warrant was issued almost three years later. Christie argued the warrant failed to meet the particularity requirement of the Fourth Amendment. The warrant sought 1) all photographs of Christie's deceased daughter; 2) all correspondence and/or documents relating to her deceased daughter; 3) all records and information including any diaries or calendars, showing the day-to-day activities of Christie and/or her deceased daughter; and 4) all addresses and/or contact information of friends, family, or acquaintances who may have had regular contact with Christie and/or her deceased daughter.[105] Though the defendant argued that Paragraph 3 allowed law enforcement to search "any and all records and information on her computer for any and all purposes," the Tenth Circuit upheld the warrant.[106]

The Tenth Circuit Court acknowledged, "an unreasonable delay in obtaining a search warrant can sometimes violate the Fourth Amendment."[107] The court determined that the totality of the circumstances must be considered with this type of case, as there are justifications for delays in various cases.

Though the court determined Christie suffered an invasion of her Fourth Amendment interests due to the delay, even though the computer itself was co-owned (though not co-used) by her and her husband.[108] Her husband consented to the seizure, and Christie neglected to raise an objection to the seizure at any time

102. *Id.* at 1160.

103. *Id.* at 1161. The Tenth Circuit Court of Appeals explained that the evidence presented at trial against Christie came from the computer "she so prized." The language shows that this opinion was governed, at least in part, by emotion.

104. *Id.* at 1162.

105. *Id.* at 1165.

106. *Id.*

107. *Id.* at 1162.

108. *Id.* at 1163.

following in the case. Thus, the court determined the government could assume any Fourth Amendment interests in the computer's continued seizure "had been voluntarily relinquished."[109] In balancing the interests, the court reasoned Christie's "interests" were not harmed considering her husband's express consent and her lack of objection. The court noted that had Christie objected, or had the husband not voluntarily relinquished the computer, the outcome may have been different.

As stated above, Christie's objection to the second warrant concerned the degree of particularity contained within the search warrant. The court notes that there is little doubt that "the particularity requirement and its underlying purposes are fully engaged when investigators seek to search a personal computer,"[110] as a personal computer holds significant personal information.[111] The court also recognizes that computers hold and contain "the very essence of the papers and effects the Fourth Amendment was designed to protect."[112] Computers, to the Tenth Circuit, are vulnerable to "rummaging" by the government.[113] In the Tenth Circuit, efforts to apply the Fourth Amendment particularity requirement to computer searches are relatively new. However, courts have held that warrants with no discernable limiting principle are invalid. Warrants may pass the particularity test if they limit their scope to either "evidence of specific federal crimes or to specific types of material."[114] In *Christie* the "non-particular" cases cited by the court were two other computer crime cases. The "sufficiently particular" cases cited by the Court were three child pornography cases.[115] Because the opening paragraph of the search warrant read "all records and information relating to the murder, neglect, and abuse of [deceased daughter]," the Court determined the warrant was sufficiently particularized, especially in light of the child pornography cases cited.[116]

---

109. *Id.*

110. *Id.* at 1164.

111. The court discusses the matter as if Christie's computer was her own, and not one co-owned by her and her husband, as was the matter discussed only a few paragraphs away in the same decision. The court could dismiss Christie's argument by employing the same reasoning as it did for the first search warrant that was analyzed – the computer was co-owned, and therefore any interest she had in the computer, and its contents were voluntarily relinquished by her husband. Instead, the court continues with the following analysis.

112. *Christie*, 717 F.3d at 1164.

113. *Id.*

114. *Id.* at 1165.

115. *See* States v. Brooks, 427 F.3d 1246, 1251 (10th Cir. 2005); United States v. Campos, 221 F.3d 1143, 1147 (10th Cir. 2000); United States v. Burke, 633, F.3d 984, 992 (10th Cir. 2011).

116. Though again, interestingly, the court does not explain how personal information such as diaries or calendars, or even photographs, may relate to abuse, murder or neglect.

On appeal, Christie argued warrants for computers should specify "limitations [on] not just *what* the government may search but *how* the government should go about its search."[117] Citing prominent child pornography cases, the court reasoned that it would be difficult to square this demand with existing case law—the child pornography cases themselves suggest that a "what" may be particular enough.[118] In fact, the Tenth Circuit has suggested that "it is unrealistic to expect a warrant to prospectively restrict the scope of a search by directory, filename or extension or to attempt to structure search methods—that process must remain dynamic."[119] The court reasoned current case law and the Fourth Amendment allow for an examination of the reasonableness of a search (allowing for a "how") given the totality of the circumstances on a case-by-case basis. Christie had the burden to show that the government was unreasonable or insufficiently particular. The court held that she did not make that showing.[120]

B. UNITED STATES V. ULBRICHT: DRUG DEALERS AND HIDDEN TRAPS

As detailed, in Part II above, law enforcement authorities went to great lengths to capture Ross Ulbricht. In his suppression case, Ulbricht argued that six separate warrants relating to servers located in Pennsylvania were unconstitutionally general. These warrants specifically concerned those leading to Ulbricht's laptop computer, his Facebook account, and his Gmail account.[121] Ulbricht never conceded that he created Silk Road, that he administered or oversaw its operations, or that he used or accessed the website.[122] He also never submitted a declaration or affidavit testifying to any personal interest in the items that were the subject of the proceeding. He instead argued that his expectation of privacy in his laptop and Google and Facebook accounts were "manifest."[123]

The Southern District of New York began its analysis of Ulbricht's personal privacy interest by quoting *Rakas v. Illinois*: "[c]apacity to claim the protection of the Fourth Amendment depends . . . upon whether the person who claims the protection of the Amendment has a legitimate expectation in the invaded place."[124] Thus, the court reasoned the law leaves "no doubt" that

117. *Christie*, 717 F.3d at 1166.
118. *Id.*
119. United States v. Burgess, 576 F.3d 1078, 1093 (10th Cir. 2009).
120. *Christie*, 717 F.3d at 1179.
121. United States v. Ulbricht, No. 14-CR-68 KBF, 2014 WL 5090039, at *1 (S.D.N.Y. Oct. 10, 2014).
122. *Id.*
123. *Id.*
124. *Id.* at 5 (quoting Rakas v. Illinois, 439 U.S. 128, 143 (1978)).

Fourth Amendment protections are based on a personal and subjective expectation of privacy.[125] To claim an interest in this thing or place, one must make an affirmative statement or declaration seeking to vindicate that interest in the place or thing to be searched. In this case, Ulbricht did not claim an interest to the property searched and seized, and for good reason: "if the government must prove any connection between himself [Ulbricht] and Silk Road" he would be required "to concede such a connection to establish his standing."[126] In other words, under current Fourth Amendment jurisprudence, Ulbricht cannot challenge the search and seizure of his personal affects without explicitly stating they are his—even if the things themselves are labeled with his identity.

The court noted that it could not proceed with a Fourth Amendment analysis in the absence of this explicitly stated or claimed interest. Even if the information contained on the Facebook and Gmail accounts were password protected, the accounts themselves involve disseminating information to others. As noted by the court, "it is also possible for more than one individual to have access to a single shared Facebook or Gmail account."[127] Simply sending an email to another person can destroy an expectation of privacy. Here, it does not matter that those things are "manifestly" Ulbricht's.[128] To gain the protections of the Fourth Amendment one must claim a privacy interest.

Ulbricht's case also involved the particularity of the warrants used against his property. Similarly to *Christie*, the court notes that just because the warrants sought to seize the entirety of the laptop they did not transform the warrants into "general" or improperly particularized warrants.[129] The warrants sought a litany of "specific" evidence, including:

> evidence of aliases, evidence concerning attempts to obtain fake identification, writings which can be used as stylistic comparisons for other "anonymous" writings, evidence concerning Ulbricht's travel patterns or movement, communications with co-conspirators regarding specified offenses, evidence concerning Bitcoin in connection with the specified offenses, and other evidence relating to the specified offenses.[130]

An individual is left unsure as to whether the search warrant

125. *Id.* at 11.
126. *Id.*
127. *Id.* at 13.
128. *Id.*
129. *Id.* at 14.
130. *Id.*

specified where this evidence could be, or in what format. Regardless, the court analogizes a computer to a home or an office: "warrants have long allowed searching a house high and low for narcotics . . . this case simply involves the digital equivalent of seizing the entirety of a car to search for weapons located within it, where the probable cause for the search is based on a possible weapons offense."[131] Thus, looking through the entire computer was held legal. The court particularly noted that electronic communications and media pose a "different set of issues."[132] Again, as in *Christie*, electronic media can be easily hidden and manipulated. As the judge in *Christie* noted, "it is rare that drug dealers point out the hidden trap in the basement."[133]

V. IS BALANCE POSSIBLE IN LIGHT OF CASES THAT EMOTIONALLY ABROGATE?

How could the government allow such results in search and seizure cases? The answer lays in the subject matter of those cases. Reason, as academics like Professor Pierre Schlag have argued, has its limits.[134] A "limit" is illustrated clearly in the *Christie* case: the court had five cases to consider when determining whether the search warrant against Christie's computer was overly broad. Two of those cases were non-child pornography related. Three of those cases related to child pornography. As discussed earlier, the court chose to follow the child pornography cases. In *Christie*, the limit, at least in part, became emotion—fear that a technologically sophisticated defendant might abuse lenient Fourth Amendment laws. Thus, reason disappears, and is replaced, or superseded by emotion:

> Reason is [thus] an essential aspect of the rule of law. It is the mechanism by which emotions, interest, and force are supposedly kept in check. In legal analysis, any time that reason is perceived to break down, the rule of law is immediately threatened. . .The fear of losing reason is a fear of loss of control. This is in part why the prospect of reason running out is such a dread moment. In the understanding

131. *Id.*

132. *Id.* at 15. (The court does not specify what these different set of issues are).

133. *Id.* at 14.

134. Professor Schlag notes that "when some choice must be made between X and X and reason supports both sides," we encounter a moment when reason is not able to provide answers in the law. PIERRE SCHLAG THE ENCHANTMENT OF REASON xxvi (Duke University Press 1998). Professor Schlag continues "[o]ne of the most interesting and least examined moments in American law is indeed the moment when reason runs out." *Id.* at 12. Reason runs out at the moment of impasse, or "as it dawns on everyone that no argument could possibly be adequate to the issue at hand." *Id.*

> of legal actors, once reason is no longer in control of an official decision-maker, arbitrariness, emotion, self-interest, politics, power, and force take over the legal machinery. From the prospective of the rule-of-law ideal, the exhaustion of reason is tantamount to an admission that legal actors do not know what they are doing—that law is, in a word, lawless.[135]

The reasoning of the above cases, rather than the actual rule of law, determined the lengths to which the court would go to justify the search and seizure of a computer in an emotional case, with the most vulnerable of victims.

The Fourth Amendment creates certain rights pertaining to search and seizure that are to be well guarded and protected for every citizen of the United States. However, when the law reaches its end[136] or an intolerable result, jurists must employ certain arguments to justify their abrogation or changing of those constitutionally bestowed rights. We find the same (or at the very least, similar) reasoning applied in cases like those of Ross Ulbricht. The distribution of illicit drugs and materials poses too great a threat to go unchecked by the law and courts. Drug dealers, like child pornographers, negatively impact society, and are presumed to be well-versed in their crimes, ready to conceal them as soon as they are caught. A similar form of emotional (or perhaps indignant) reasoning is found in Rebecca Christie's case, where mother's addiction for her computer led to the neglectful and horrific death of her three-year-old child.

The lengths to which the Tenth Circuit Court went to distinguish *Christie* again demonstrates that the law must make choices—choices that may abrogate rights—when there is a potentially intolerable result to an emotionally charged or horrifying case. *Christie* cited two cases that arguably demonstrated how the search warrant was overly broad. However, the court chose to follow three child pornography cases, which came out at the opposite result. Thus, using those child pornography cases, the Tenth Circuit could find that the warrant was not overly broad simply because it had some degree of particularity and certainty pertaining to what was to be searched.[137]

---

135. Schlag, *supra* note 134, at 20–21.

136. *Id.* at 128.

137. A large part of the issue is that Tenth Circuit child pornography case law does not require or demand "technical precision" in computer-related search warrants. United States v. Christie, 717 F.3d 1156, 1165 (10th Cir. 2013). In *Christie*, the court reasoned that because law enforcement was restricted by the preamble to the search warrant to search only for evidence of neglect, they could not look for just *anything* on the computer. *Id.* at 1165-66. It is difficult to conceptualize how one might accomplish this task. For example, a law enforcement officer must open each document on a

The concern that the government may be able to search every iota of information in a computer is well founded given the above explored child pornography cases, especially in the *Christie* decision. Also concerning is the fact that it is unclear how the computer showed that Christie was neglecting her child. The district attorney and trial court demanded a log of her World of Warcraft account activities, demonstrating that she was playing the game when she should have been caring for her child. In other words, it is unclear why they seized her computer.[138] The court assumes that Christie was unsophisticated enough to leave evidence of child neglect (via images, documents, and diaries) on her computer, but at the same time sophisticated enough to be able to manipulate or hide that evidence.

Certainly, no citizen wants child pornographers, neglectful mothers, or drug dealers to avoid punishment for their crimes because of their ability to manipulate technology or because of loopholes in the law that require strict particularity.[139] However, the current trend of Fourth Amendment search and seizure law as applied to computer crimes cannot continue. Emotional abrogation of rights considering the ever growing and adapting child pornography industry certainly makes sense. But, what of these other computer crimes—crimes like Christie's do not involve a computer per se, but are only tangentially related?

Computers are involved in almost every aspect of an American citizen's life. For many, computers, tablets, and cell phones are their lifeblood, used to keep calendars, recipes, notes, diaries, games, photographs and work documents. The current case law puts personal documents at risk if the owner is accused of a crime. This is especially apparent in Ulbricht's case. Though Ulbricht never claimed to have owned or created Silk Road, he did claim at least some sort of "manifest" interest in his Facebook account, Gmail account, and personal laptop. Because Ulbricht did not explicitly claim these things as his own, however, the FBI

computer with the intent of finding evidence of neglect, but therein lies the issue—they must look through every, single, document.

138. The court in *Christy* did not clarify what, if any, evidence of neglect was found on the computer, other than the computer itself. This creates a bizarre trial strategy. For example: imagine a depressed mother who cannot leave her couch. Because she is depressed, she neglects her small child and the child dies. The prosecutor would not see fit to seize and search her couch as evidence of abuse. Christie's use of a computer as a vehicle to neglect her child made the court especially indignant, and more willing to seize it, though it might not have rendered any further useful evidence of the crime committed.

139. Evidenced in *Christie*, government and law enforcement agencies fear defendants and criminals will abuse potentially lenient Fourth Amendment case law to manipulate files on computers to avoid prosecution: "[c]omputer files can be misnamed by accident, disguised by intention, or hidden altogether, leaving investigators at a loss to know *ex ante* what sort of search will prove sufficient to ferret out the evidence they legitimately seek." *Christie*, 717 F.3d at 1166 (10th Cir. 2013).

could seize them. The documents on them were used to build evidence against him and connect him to Silk Road (primarily by analyzing stylistic comparisons in writings). As such, even completely unrelated documents or items on a computer are at risk. The further search and seizure of unrelated items may be defended by the state with any number of doctrines, such as plain view, exigent circumstances, inevitable discovery, and good faith.

In preventing certain villainous defendants from abusing loopholes in search and seizure law the government created its own loopholes. The problem is that these governmental loopholes do not just serve the ends of justice and protection of vulnerable victims—they potentially affect every citizen who uses computers on a regular basis. The concern is apparent in an age where citizens grow increasingly aware and concerned about government intrusion on and surveillance of Internet activities.[140] Moreover, the case law and reasoning suggests that citizens who use technology have some sort of capacity for manipulation. The courts' reasoning in *Christie* and *Ulbricht* suggest that anyone can manipulate or hide certain illicit or illegal documents or files on a computer without any substantial information to back up that claim or fear.[141] While there is awareness as to the impermissible monitoring the government may be imposing on citizens, everyday citizens may not realize that surveillance of their Internet and computer activities can be used to justify a search of not only their computers, but also their entire home.

Given the willingness of certain courts (like the *Christie* court) to cite child pornography cases in computer search and seizure cases, it does not seem at first blush that balance is possible. Courts may be too willing to blindly follow reason—reason that was originally informed by emotion[142] and a need to overcome intolerable results in criminal cases with extremely vulnerable victims. However, it seems that a "how" to search in computer search and seizure cases is not as difficult as a "what" to search, particularly in cases that do not concern child pornography, where the defendants tend to be well-versed in the crimes and how to conceal them. Perhaps courts should distinguish such cases. Courts could plausibly apply a strict level of analysis to their ex-post findings in search and seizure

140. *See* Anne Flaherty, *Study Finds Online Privacy Concerns on the Rise*, NEWSOK (Sept. 5, 2013, 12:39 AM), http://newsok.com/article/feed/586914 [https://perma.cc/4GZ4-UCLT].

141. Other than experience with, and research about child pornographers and their abilities to manipulate documents and files on a computer via such avenues as encryption.

142. Particularly sadness, and fear that crime will spread, especially given the explosion of technology in recent years.

appellate cases.[143] Were the categories in Christie's case too broad? What do her personal diaries and calendars have to do with the same? Especially diaries and calendars spanning a timeline of four years?[144]

CONCLUSION

After researching the history of child pornography and other computer crime statues, one can easily become concerned with the ability of courts to impermissibly abrogate Fourth Amendment rights under the current case law involving the search of computers. Under the current legal scheme of the Wiretap and Pen/Trap statutes, the government need not attest to how it gathers facts justifying a search and seizure, nor does the government need to specify the "what" to be seized and searched. Thus, if an individual is prosecuted under one of the statutes, that individual cannot argue protection against search and seizure as far as probable cause, nexus, and particularity goes. While it is hard to identify and sympathize with the prolific criminals explored above, the potential of these statues and the case law to impact the lives of citizens is concerning. The development of Fourth Amendment search and seizure jurisprudence in computer crime cases demands an inquiry as to whether prevention of technologically related crime is worth these abrogative risks.

Computer crime cases are on the rise, but courts often find themselves at a loss as to how to deal with the search and seizure of computers when they are used in a crime. Many courts find themselves trying to cite cases that have little to do with computer crimes. Because there is little case law regarding computer crimes and few salient analogues for courts to use in their reasoning, the case law must develop within a vacuum or void. Herein lies the risk: that emotion, politics, or force (as cited by Professor Schlag) may precede, or even supersede sound legal reasoning in these cases. Courts must tread lightly in this developing area of law.

143. Such endeavors have been taken in other jurisdictions including the Ninth Circuit. In United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010), the court bound the government to a strict set of guidelines when searching a database to determine whether Major League Baseball players tested positive for steroid use. Though the Ninth Circuit pulled back on the district court's recommendations, the challenged warrants still needed to meet particularity requirements as compared to the Christie case.

144. Or, perhaps on the other hand, the concerns of law enforcement agencies and the government are valid. Computers, widespread and pervasive in our society, can be easily manipulated and abused for crime—crimes that may impact not only vulnerable victims like those of child pornography, child neglect, and drug trafficking, but those of identity theft and fraud as well.