Warrantless Searches of Computers and Other Electronic Devices

Jeff Welty

School of Government

April 2011

I. REASONABLE EXPECTATION OF PRIVACY

The first step in determining whether there has been an improper warrantless search of a defendant's computer or other electronic device is determining whether there has been a search at all, i.e., whether the defendant had a reasonable expectation of privacy in the contents of the device. The vast majority of cases to have considered this issue have held that individuals do have a reasonable expectation of privacy in the contents of their own electronic devices. The cases below consider the existence of a reasonable expectation of privacy in unusual circumstances that raise doubts about the existence of such an expectation.

A. WORKPLACE AND SCHOOL COMPUTERS AND DEVICES

City of Ontario v. Quon, __ U.S. __, 130 S.Ct. 2619 (2010) (Court assumes arguendo that police officers had a reasonable expectation of privacy in department-issued pagers, but notes that "employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated")

United States v. Heckenkamp, 482 F.3d 1142 (9th Cir. 2007) (student retained reasonable expectation of privacy in computer despite the fact that he connected it to the school's network where there was no announced policy of monitoring, and instead, users were told that there would be only "limited instances in which university administrators may access [a user's] computer in order to protect the university's systems")

United States v. Finley, 477 F.3d 250 (5th Cir. 2007) (defendant had a reasonable expectation of privacy in a cell phone that his employer provided for him)

United States v. Ziegler, 474 F.3d 1184 (9th Cir. 2007) (defendant had a reasonable expectation of privacy in his work computer because it was located in an individual office, despite company policy allowing monitoring of the computer)

United States v. Barrows, 481 F.3d 1246 (10th Cir. 2007) (employee had no reasonable expectation of privacy in his personal computer after he brought it to work, connected it at least to some degree to the workplace network, used it in an exposed area, and left it on, with no password protection, when he was away from his desk)

United States v. Angevine, 281 F.3d 1130 (10th Cir. 2002) (university professor had no reasonable expectation of privacy in computer owned by the university but issued to the professor, where the university's policy "explicitly cautions computer users that information flowing through the [u]niversity network is not confidential either in transit or in storage on a [u]niversity computer")

United States v. Simons, 206 F.3d 392 (4th Cir. 2000) (employee had no reasonable expectation of privacy in work computer where employer's policy indicated that Internet use would be monitored and therefore "placed employees on notice that they could not reasonably expect that their Internet activity would be private")

B. USE OF FILE-SHARING SOFTWARE

State v. Bailey, 989 A.2d 716 (Me. 2010) (although defendant used P2P file-sharing software, he maintained a reasonable expectation of privacy in the files against access by means other than a file-sharing network – specifically, against a police officer who accessed the files by searching the defendant's computer)

United States v. Borowy, 595 F.3d 1045 (9th Cir. 2010) (follows Ganoe, infra)

United States v. Stults, 575 F.3d 834 (8th Cir. 2009) (defendant had no reasonable expectation of privacy in computer on which he had installed P2P file-sharing software, and agents' use of such software to examine the contents of the defendant's computer and to copy images of child pornography from the computer was not a search)

United States v. Ganoe, 538 F.3d 1117 (9th Cir. 2008) (defendant had no reasonable expectation of privacy in the contents of a computer on which he had installed file-sharing software: "Although as a general matter an individual has an objectively reasonable expectation of privacy in his personal computer. . . we fail to see how this expectation can survive Ganoe's decision to install and use file-sharing software, thereby opening his computer to anyone else with the same freely available program.")

United States v. King, 509 F.3d 1338 (11th Cir. 2007) (similar to Ganoe and Stults)

C. STOLEN COMPUTERS AND DEVICES

United States v. Caymen, 404 F.3d 1196 (9th Cir. 2005) (defendant had no reasonable expectation of privacy in computer that he obtained by fraud: "The Fourth Amendment does not protect a defendant from a warrantless search of property that he stole.")

Hicks v. State, 929 So.2d 13 (Fla. Ct. App. 2006) (defendant had no reasonable expectation of privacy in stolen computer and so officers' search thereof did not violate the Fourth Amendment)

D. INTERESTING OUTLIERS REGARDING CALL LOGS

United States v. Maldonado, 2009 WL 2760798 (D. Kan. Aug. 26, 2009) ("Just as there is no reasonable expectation of privacy in numbers called or numbers calling, because they are voluntarily turned over to third parties, see Smith v. Maryland, 442 U.S. 735 (1979), there may be no reasonable expectation of privacy in a cell phone's recent call directory or phonebook directory.")

United States v. Fierros-Alavarez, 547 F.Supp.2d 1206 (D. Kan. 2008) (defendant had no reasonable expectation of privacy in call log and address book, as dialed and received call information is shared with the phone company and address book contained nothing more than names and phone numbers similar to that in the call log)

E. LOST, ABANDONED, AND MISLAID PROPERTY

People v. Schutter, __ P.3d __, 2011 WL 1106768 (Colo. Mar. 28, 2011) (defendant who accidentally locked his iPhone in a gas station restroom, leading a gas station employee to turn it over to police, did not abandon the phone; and even if "an otherwise reasonable expectation of privacy . . . is diminished when that property is lost or mislaid because it is only reasonable to expect that an officer . . . will examine it to learn how it can be returned to its owner," there was no need for an officer to examine the phone in this case, because the defendant knew where he had left it, but had not yet returned to retrieve it)

State v. Dailey, 2010 WL 3836204 (Ohio Ct. App. 3 Dist. Oct. 4, 2010) (defendant "voluntarily abandoned his cell phone when he slipped out of his coat and left it and its contents [including the phone] behind in order to escape being detained" for shoplifting by a loss prevention employee of a retail store)

United States v. Crist, 627 F.Supp.2d 575 (M.D. Pa. 2008) (defendant owned a computer which he kept in a house he rented; he did not stay current on the rent and allowed the house to fall into squalor, leading the landlord to hire a crew to move the defendant's property, including the computer, out of the house, though the landlord did not commence formal eviction proceedings; the defendant's actions did not constitute abandonment of the computer)

II. PRIVATE SEARCHES

Even when a defendant has a reasonable expectation of privacy in a computer or other electronic device, if that expectation of privacy is violated by a private actor rather than a government entity, there is no Fourth Amendment violation. See, e.g., United States v. Grimes, 244 F.3d 375 (5th Cir. 2001) (computer repair technician searched defendant's computer and found child pornography; the search "being private in nature, is not subject to Fourth Amendment analysis"). The so-called private search doctrine comes up regularly with respect to computers, but the issues it presents in this context are not different than in other settings, so I have not attempted to collect cases on point.

III. CONSENT SEARCHES

Assuming that a defendant has a reasonable expectation of privacy in a computer or an electronic device, and that the police do not have a valid warrant authorizing a search of the device – warrant searches are beyond the scope of this manuscript – the issue becomes whether one of the several exceptions to the warrant requirement applies. The remainder of this document collects cases on the various exceptions, starting with consent.

A. CELLULAR PHONES

1. SEARCHES WITHIN SCOPE OF CONSENT

Lemons v. State, 298 S.W.3d 658 (Tex. Ct. App. – Tyler 2009) (officers asked defendant if he had been talking to a minor on his cell phone; shortly thereafter, an officer asked to see defendant's cell phone and defendant handed him the phone; after looking at the call log, the officer accessed the phone's camera feature

and saw a nude picture of the minor; appellate court rejects defendant's argument that by looking at the picture, the officer exceeded the scope of the defendant's consent)

Guy v. State, 913 A.2d 558 (Del. 2006) (defendant consented to a "complete and thorough search" of his apartment, and stood silently by as officers searched his pager; the search was within the scope of the defendant's consent)

People v. Berry, 731 N.E.2d 853 (Ill. Ct. App. 2000) (officer asked defendant, in the course of discussing the ownership of defendant's cellular phone, "mind if I take a look at [your phone]," and defendant said "go right ahead"; this was sufficient to allow officer to turn phone on, at which point, officer immediately noted incriminating data)

2. SEARCHES OUTSIDE SCOPE OF CONSENT

United States v. Zavala, 541 F.3d 562 (5th Cir. 2008) (officers suspected defendant of drug trafficking; executed Terry stop of defendant's car; placed defendant's cell phone on the roof of the car; got defendant's consent to search the car; consent did not extend to cell phone)

Smith v. State, 713 N.E.2d 338 (Ind. Ct. App. 1999) (officers asked for and received consent to search defendant's vehicle for guns, drugs, money, or illegal contraband; they seized two cellular phones, and by partially disassembling them, determined that they were "cloned," i.e., modified so that the charges would be billed to someone other than the user; trial and appellate courts ruled that the search exceeded the scope of defendant's consent, because guns, drugs, etc., were not likely to be found in the phones)

3. WHO MAY CONSENT

United States v. Meador, 2008 WL 4922001 (E.D. Mo. Jan. 7, 2008) (unpublished) (murder suspect's mother had apparent authority to consent to search of vehicle owned by her husband but driven by her son; however, she did not have any authority to consent to the search of a cellular phone registered to her husband's account but used by her son)

B. COMPUTERS

1. SEARCHES WITHIN SCOPE OF CONSENT

United States v. Luken, 560 F.3d 741 (8th Cir. 2009) (officers suspected the defendant of possessing child pornography and asked for consent to search his computer; he agreed in writing, authorizing the officers to "seize and view" his computer; the officers seized the computer, and one of them later examined its contents using special forensic software, finding child pornography; the defendant moved to suppress, arguing that the comprehensive forensic examination conducted by the officer went beyond "view[ing]" the computer, but neither the trial court nor the appellate court agreed, in part because the officers told the defendant prior to the search that they had access to forensic tools that allowed them to recover deleted files, etc.)

United States v. Lucas, 2008 WL 4858185 (W.D. Ky. Nov. 7, 2008) (unpublished) (holding that a search of defendant's non-password-protected computer was within the scope of his consent, which authorized officers to search his home for "other material and records pertaining to narcotics")

United States v. Wells, 2008 WL 2783264 (S.D. Iowa July 15, 2008) (unpublished) (defendant's wife consented to search of their home for "illegal drugs, drug paraphernalia, pipes, scales, [baggies], large amounts of cash, logs, notebooks, ledgers, [and] records related to drug sales"; officers searched defendant's computer and saw several images of child pornography; court denied motion to suppress because the scope of the wife's consent included permission to "search for documents relating to drug trafficking," which "could easily be stored on a computer and could be in a .jpg or .pdf file")

United States v. Sloan, 2007 WL 1521434 (D. Hawai'i May 22, 2007) (unpublished) (consent to "seize [a] computer as evidence" permitted officers to search the computer for child pornography, where the consent was given in the context of the officers' questioning the defendant about his possession of child pornography and his use of a computer to receive and distribute it)

United States v. Brooks, 427 F.3d 1246 (10th Cir. 2005) (officers told defendant that they were investigating him for possession of child pornography; he signed a consent to a "complete search" of his computer; although the officers told the defendant that they would use a "pre-search" disk, they ended up doing a manual search instead; although the method used for searching was different than the one explained to the defendant, the search was still permitted under the defendant's broad consent)

United States v. Long, 425 F.3d 482 (7th Cir. 2005) (defendant consented to a search of his office and computer; the fact that officers used forensic software to search the computer did not cause the search to be beyond the scope of his consent)

United States v. Rossby, 81 Fed. Appx. 109 (9th Cir. 2003) (unpublished) (holding that a search of defendant's non-password-protected laptop computers was within the scope of his consent, which authorized officers to conduct a "complete search" of his office and to take "from my premises any letters, papers, materials, or other property which they may desire")

United States v. Al-Marri, 230 F.Supp.2d 535 (S.D.N.Y. 2002) (defendant's consent to search of his home inherently included consent to search containers, including a computer, within the home; scope of consent was particularly clear here, where defendant, upon request, unplugged the computer and handed it to the officers)

United States v. Greene, 56 M.J. 817 (N. M. Ct. Crim. App. 2002) (officers did not exceed scope of consent, which allowed them to search defendant's residence and remove and retain items therein, simply by keeping a seized computer for three months to conduct a detailed examination of it)

2. SEARCHES OUTSIDE SCOPE OF CONSENT

State v. Bailey, 989 A.2d 716 (Me. 2010) (officer who suspected defendant of possessing child pornography asked for permission to search his computer for evidence of intrusions; defendant consented; officer then searched all video files on the computer, finding child pornography; consent was voluntary notwithstanding the officer's deception, but the officer's search exceeded the scope of consent because a search for evidence of intrusions would not naturally include an examination of video files)

State v. Prinzing, 907 N.E.2d 87 (Ill. Ct. App. 2009) (officers told the defendant that they believed that he may have been the victim of fraudulent credit card charges and asked to search his computer for evidence of the fraud, including computer viruses; the defendant agreed, and the officers then searched the computer, finding images of child pornography; the defendant moved to suppress, arguing that he gave the officers consent to search for viruses and evidence of credit card fraud, and that his consent did not include consent to look at image files, which would not be likely to contain the things for which the officers said they wanted to look; although the trial court denied his motion, the appellate court reversed, finding that the officers exceeded the scope of the defendant's consent)

United States v. Osorio, 66 M.J. 632 (A.F. Ct. Crim. App. 2008) (defendant consented to search of an external hard drive when officers indicated that they wanted to see pictures he had taken at a party at which a sexual assault took place; officers later searched for, and found, child pornography; appellate court ruled that the search exceeded the scope of defendant's consent)

United States v. Richardson, 583 F.Supp.2d 694 (W.D. Pa. 2008) (holding that a search of defendant's hard drive for child pornography exceeded the scope of defendant's consent, which was given in the context of a discussion of possible illegal use of the defendant's credit card, i.e., of the defendant being a victim of some type of fraud)

United States v. Stierhoff, 477 F.Supp.2d 423 (D.R.I. 2007) (officers asked to search defendant's computer, indicating that they were interested in poems he wrote in connection with stalking a young woman; defendant consented, indicating that the poems were in a particular folder; officers also searched another folder, labeled "offshore," and found evidence of tax evasion; search of the "offshore" folder exceeded the scope of defendant's consent, which was limited by the expressed object of the search)

United States v. Carey, 172 F.3d 1268 (10th Cir. 1999) (officers suspected defendant of drug activity and obtained his consent to a "complete search of the premises and property" where he lived; the officers seized and searched a computer, finding evidence of child pornography; the defendant's general consent to the search of his apartment did not authorize a search of the computer)

United States v. Turner,169 F.3d 84 (1st Cir. 1999) (defendant called the police to report seeing an intruder in a neighbor's apartment; the neighbor reported a sexual assault; after officers noticed that defendant's window screen was ajar, they asked to search defendant's apartment for evidence that the intruder had been in defendant's apartment as well; defendant gave consent; during the search, the officers began to suspect that the defendant was the assailant; after noticing a sexual screen saver on defendant's computer, one officer began to search it, locating child pornography; defendant later moved to suppress, and the First Circuit ruled that the search exceeded the scope of the defendant's consent, which was limited to a search for evidence that an intruder had been in his apartment)

3. WHO MAY CONSENT

United States v. Stabile, 633 F.3d 219 (3rd Cir. 2011) (consent of woman who was living with, and who thought that she was married to, defendant was sufficient to allow officers to seize and search defendant's computers; factors relevant to determining common authority include "the identity of the user(s), whether password protection is used, and the location of the computer in the house"; although defendant arrived as the officers were leaving and stated "I take it [her consent] back," this had no legal effect)

United States v. Jackson, 598 F.3d 340 (7th Cir. 2010) (defendant's mother had apparent authority to consent to search of computer case belonging to defendant where officers saw the defendant give his mother the case and she stated that he gave it to her so that she could download pictures of her grandchild)

United States v. Hudspeth, 518 F.3d 954 (8th Cir. 2008) (wife's consent to search of shared computer was valid even though (1) husband, who was not present, had previously refused consent, and (2) officers did not tell wife of husband's refusal)

United States v. Buckner, 473 F.3d 551 (4th Cir. 2007) (wife had apparent authority to consent to search of computer that she leased and that was located in a common area of the home she and her husband shared; although husband had password-protected files, the officer who conducted the search did not know that they were password-protected, because no one told him so, and because, by creating a forensic image of the hard drive, he bypassed any passwords)

Trulock v. Freeh, 275 F.3d 391 (4th Cir. 2001) (one user of a shared computer has no authority to consent to a search of password-protected files belonging to another user)

IV. SEARCHES INCIDENT TO ARREST

When a suspect is arrested, the suspect and his "grab space" may be searched thoroughly, as a means of ensuring officer safety and preventing the destruction of evidence.

A. CELLULAR PHONES

1. SEARCH PERMITTED

United States v. Curtis, 635 F.3d 704 (5th Cir. 2011) (upholding search of cell phone incident to arrest based on United States v. Finley, 477 F.3d 250 (5th Cir. 2007), stating that the Fourth, Seventh, and Tenth Circuits [the Tenth Circuit case it cites is unpublished] also allow such searches, and declining to address whether Arizona v. Gant, __ U.S. __, 129 S.Ct. 1710 (2009), may limit searches of cell phones incident to arrest)

People v. Diaz, 244 P.3d 501 (Cal. 2011) (search of cell phone 90 minutes after arrest was permissible; it was taken from the arrestee's immediate person, and the "sheer quantity of personal information" contained therein was irrelevant)

State v. Wilkerson, 363 N.C. 382 (2009) (holding, with little discussion, that "the seizure and the search of the telephone were properly accomplished pursuant to a lawful arrest")

United States v. Murphy, 552 F.3d 405 (4th Cir. 2009) (upholding search of cell phone incident to arrest because call logs and text messages are volatile, i.e., evidence may disappear as new calls and text messages are received)

United States v. Wurie, 612 F.Supp.2d 104 (D. Mass. 2009) (upholding search of cell phone incident to arrest and collecting cases)

United States v. Santillan, 571 F.Supp.2d 1093 (D. Ariz. 2008) (upholding search of cell phone incident to arrest; alternatively, the search was valid under the exigent circumstances doctrine, because of the risk that incoming calls and text messages would crowd out calls and text messages of evidentiary value)

United States v. Ortiz, 84 F.3d 977 (7th Cir.1996) (upholding search of a pager incident to arrest because of the device's finite memory and the potential for new messages crowding out existing ones)

2. SEARCH NOT PERMITTED

State v. Smith, 920 N.E.2d 949 (Ohio 2009) (searches incident to arrest are justified to preserve evidence and to ensure officer safety, but neither purpose is served by searching a cell phone that has been secured; cell phones are not like other "containers" because (1) they do not contain other physical objects and (2) they may store a "wealth" of personal information; therefore, without a warrant, officers may take steps to preserve data in a cell phone, but may not search it absent an officer safety concern or exigency; exigency by "crowding out" was not established in this case, and in any event, the service provider may be able to provide call log information)

United States v. McGhee, 2009 WL 2424104 (D. Neb. July 21, 2009) (relying on Gant to invalidate a search of the defendant's cell phone incident to arrest)

United States v. Quintana, 594 F.Supp.2d 1291 (M.D. Fla. 2009) (defendant arrested for driving on a suspended license; because his car smelled of marijuana, police also suspected drug activity; search of cell phone incident to arrest improper because the search "had nothing to do with officer safety or the preservation of evidence related to the crime of arrest," but rather was a fishing expedition for evidence of drug activity)

United States v. Wall, 2008 WL 5381412 (S.D. Fla. Dec. 22, 2008) (unpublished) (holding that cell phones may not be searched incident to arrest, as the contents of a cell phone present no risk of danger to the arresting officers, and because "searching through information stored on a cell phone is analogous to a search of a sealed letter, which requires a warrant")

United States v. Park, 2007 WL 1521573 (N.D. Cal. May 23, 2007) (unpublished) (holding that a search of an arrestee's cell phone 90 minutes after the arrest was not sufficiently contemporaneous with the arrest)

B. COMPUTERS

1. SEARCH NOT PERMITTED

United States v. Urbina, 2007 WL 4895782 (E.D. Wis. Nov. 6, 2007) (unpublished) (upholding search of cell phone incident to arrest, but stating in *dicta* that "[i]n the case before this court, [the officer] limited his search to the phone's address book and call history. If the evidence in a future case were to show that the warrantless search conducted by law enforcement was essentially equivalent to a search of a personal computer, without sufficient exigencies to justify such a search, the court's reaction may be different, because of the substantial invasion of privacy.")

United States v. Park, 2007 WL 1521573 (N.D. Cal. May 23, 2007) (unpublished) (invalidating search of an arrestee's cell phone 90 minutes after arrest, and noting in disapproving *dicta* that "the government asserted that, although the officers here limited their searches to the phones' address books, the officers could have searched

any information-such as emails or messages-stored in the cell phones. In addition, in recognition of the fact that the line between cell phones and personal computers has grown increasingly blurry, the government also asserted that officers could lawfully seize and search an arrestee's laptop computer as a warrantless search incident to arrest.")

State v. Washington, 2002 WL 104492 (Wash. Ct. App. Jan. 28, 2002) (unpublished) (holding, with little analysis, that officers lacked authority to search a laptop incident to arrest, even where they had probable cause to believe that the laptop was stolen)

C. EFFECT OF ARIZONA V. GANT

In Arizona v. Gant, 556 U.S. __ (2009), the Supreme Court held that an officer could search a suspect's vehicle incident to arrest only if (1) the suspect is unsecured and could reach into the vehicle, or (2) there is reason to believe that evidence of the crime of arrest may be found in the vehicle. A few cases have suggested that Gant may apply outside the vehicle context. See, e.g., United States v. Shakir, 616 F.3d 315 (3rd Cir. 2010) (luggage); United States v. Taylor, 656 F.Supp.2d 998 (E.D. Mo. 2009) (attic space) . If so, the reasoning of Gant may provide some support for the argument that once a defendant has been secured and can no longer access his computer, cellular phone, or the like, a search of the device should be permitted only if there is reason to believe that evidence of the crime of arrest may be found in the device.

V. AUTOMOBILE EXCEPTION

Because automobiles are highly mobile and because drivers have reduced expectations of privacy in automobiles as opposed to residences, automobiles in public places may be searched based on probable cause without a warrant. Such a vehicle search may extend to any location in the vehicle, including closed containers, where the object of the search may reasonably be found. United States v. Ross, 456 U.S. 798 (1982). Thus, where there is probable cause to believe that evidence of a crime may be found in a particular vehicle, it may be permissible to treat any electronic devices in the car as "containers" and to search the devices to the extent that the search reasonably might uncover evidence of the crime in question.

A. CELLULAR TELEPHONES

1. SEARCH JUSTIFIED UNDER AUTOMOBILE EXCEPTION

State v. Boyd, 992 A.2d 1071 (Conn. 2010) (applying automobile exception to uphold search of cell phone taken from the passenger seat of the car the defendant had been driving)

People v. Chho, 2010 WL 1952659 (Cal. Ct. App. 6 Dist. May 17, 2010) (unpublished) (officers obtained consent to search the defendant's car an found six ounces of marijuana; his cell phone was in the car and rang frequently; the combination of the drugs and the frequently ringing phone provided probable cause to believe that the phone would contain evidence of drug activity, and the officers properly opened it and reviewed two text messages on it under the automobile exception)

United States v. Fierros-Alavarez, 547 F.Supp.2d 1206 (D. Kan. 2008) (search of cell phone that was located inside vehicle of suspected drug trafficker justified based on vehicle exception plus probable cause to believe that the phone would contain evidence of drug trafficking)

United States v. Rocha, 2008 WL 4498950 (D. Kan. Oct. 2, 2008) (unpublished) (holding, as to cell phones found in RV in which drugs were being transported, "[b]ecause probable cause existed to believe that evidence of a crime would be found in the cell phone information, the automobile exception allows the search of the cell phones just as it allows a search of other closed containers found in vehicles")

United States v. James, 2008 WL 1925032 (E.D. Mo. April 29, 2008) (search of cell phone that was inside vehicle justified: "Because probable cause existed to believe that evidence of a crime would be found in the cell phone call records and address book, the automobile exception allows the search of the cell phone just as it allows a search of other closed containers found in vehicles.")

State v. Novicky, 2008 WL 1747805 (Minn. Ct. App. April 15, 2008) (unpublished) (search of cell phone on front seat of vehicle was justified under automobile exception; evidence of ownership of the cell phone was likely to be relevant evidence in establishing the ownership of the gun that was next to it)

United States v. Meador, 2008 WL 4922001 (E.D. Mo. Jan. 7, 2008) (unpublished) (pagers and cell phones "may be considered closed containers," and here, there was probable cause to search a cell phone that was found in a vehicle)

United States v. Woodley, 2005 WL 3132205 (E.D. Mich. Nov. 22, 2005) (unpublished) (search of pager authorized by automobile exception)

B. COMPUTERS

1. CASES RAISING, BUT NOT DECIDING, THIS ISSUE

State v. Newman, 237 P.3d 1222 (Idaho Ct. App. 2010) (laptop properly seized under vehicle exception where police had probable cause to believe that the suspect was using the computer for criminal activity; however, it was only searched after search warrants were obtained, so it does not quite reach the ultimate issue)

United States v. Burgess, 576 F.3d 1078 (10th Cir. 2009) (officers developed probable cause to believe that vehicle contained evidence of drug crimes; proper to seize computer and hard drive found therein; court declines to decide whether it was proper to search the devices under the automobile exception, instead finding that the searches were proper under a search warrant)

VI. EXIGENT CIRCUMSTANCES

The exigent circumstances exception applies when obtaining a warrant would be too time-consuming in light of a risk of danger, a risk of destruction of evidence, or some other concern.

A. CELLULAR TELEPHONES

1. SEARCH JUSTIFIED BY EXIGENT CIRCUMSTANCES

United States v. Santillan, 571 F.Supp.2d 1093 (D. Ariz. 2008) (exigent circumstances justified seizure of cell phone that defendant, a suspected "spotter" for drug traffickers, appeared to be using to help coordinate the movements of vehicles smuggling drugs; search was also justified, in order to preserve information in call log)

United States v. Zamora, 2006 WL 418390 (N.D. Ga. 2006) (unpublished) (warrantless search of cellular phones justified by exigent circumstances; similar to Parada, infra)

United States v. Parada, 289 F.Supp.2d 1291(D. Kan. 2003) ("Because a cell phone has a limited memory to store numbers, the agent recorded the numbers in the event that subsequent incoming calls effected the deletion or overwriting of the earlier stored numbers. This can occur whether the phone is turned on or off, so it is irrelevant whether the defendant or the officers turned on the phone. . . . [U]nder these circumstances, the agent had the authority to immediately search or retrieve, as a matter of exigency, the cell phone's memory of stored numbers of incoming phone calls, in order to prevent the destruction of this evidence.")

2. SEARCH NOT JUSTIFIED BY EXIGENT CIRCUMSTANCES

United States v. Morales-Ortiz, 376 F.Supp.2d 1131 (D. N.M. 2004) (stating in dicta that a search of a cell phone's address book, unlike a search of its call log, cannot be justified on the basis of an exigent need to preserve evidence, since the address book is not subject to being overwritten by incoming calls)

B. COMPUTERS

1. SEIZURE, BUT NOT SEARCH, JUSTIFIED BY EXIGENT CIRCUMSTANCES

United States v. Mitchell, 565 F.3d 1347 (11th Cir. 2009) (warrantless seizure of computer justified after defendant admitted during consensual interview in his home that it contained child pornography, but because the defendant did not consent to a search of the computer, a warrant was necessary for the search; and a 21-day delay in obtaining the warrant was excessive)

State v. Rupnick, 125 P.3d 541 (Kan. 2005) (seizure of laptop, but not search, was justified by exigent circumstances when officers had probable cause to believe that the computer contained data that the defendant had stolen from a former employer and defendant knew of officers' suspicions; he could have destroyed the data quickly and easily)

VII. OTHER EXCEPTIONS TO THE WARRANT REQUIREMENT

There are several other possible justifications for a warrantless search of a computer or another electronic device. These possible justifications appear to come up less frequently in practice, so they are treated only briefly below.

A. BORDER SEARCHES

Generally, officers may search anyone and anything coming into the United States, without a warrant or even suspicion. Several cases have upheld searches of laptop computers under the border search doctrine. See, e.g.,

United States v. Cotterman, __ F.3d __, 2011 WL 1137302 (9th Cir. Mar. 30, 2011) (defendant's laptop was seized at the border but taken 170 miles away to a laboratory and searched several days later; reversing the district court, the court upheld this search under the border search doctrine); United States v. Arnold, 523 F.3d 941 (9th Cir.2008); United States v. Romm, 455 F.3d 990 (9th Cir.2006); United States v. Ickes, 393 F.3d 501 (4th Cir.2005); United States v. Roberts, 274 F.3d 1007 (5th Cir.2001) (diskettes). Because of complaints by international business travelers concerned about the security of important business data, Congress has held hearings about border searches and has begun to consider regulating border laptop searches by statute; the Department of Homeland Security recently indicated that it would promulgate new internal standards for such searches, in what appears to be an attempt to obviate the need for legislative action. The ACLU has filed a civil suit arguing that such searches require individualized suspicion, even if not full probable cause.

B. PROBATION SEARCHES

At a minimum, warrantless searches of a probationer's computers and other electronic devices are permissible if (1) they are based upon reasonable suspicion, and (2) submission to such searches is a condition of the defendant's probation. United States v. Knights, 534 U.S. 112 (2001).

- Probationers who are subject to the warrantless search condition in G.S. 15A-1343(b)(13). It is now a standard condition of probation that a probationer must submit to warrantless searches of his "person . . . vehicle and premises" by a probation officer, at least "for purposes directly related to the probation supervision." (A probationer also must submit to certain searches by a law enforcement officer, as specified in G.S. 15A-1343(b)(14).) The quoted language appears to be broad enough that a probationer must submit to searches of his computers and other electronic devices, if the devices are in his residence, in his vehicle, or on his person, and if there is reason to suspect that they could contain evidence relevant to the defendant's supervision. Although the requirement of reasonable suspicion is not set forth in the statute, our appellate courts have appeared to endorse it in the context of searches of probationers in State v. Robinson, 148 N.C. App. 422 (2002), though that was before the 2009 amendments to the statute. Cf. United States v. Midgette, 478 F.3d 616 (4th Cir. 2007) (appearing to conclude that the statute allows suspicionless searches). As an aside, some courts have held that warrantless searches are permissible if they are based upon reasonable suspicion even if submission to such searches is not a condition of the defendant's probation. See, e.g., United States v. Yuknavich, 419 F.3d 1302 (11th Cir. 2005) (despite absence of warrantless search condition, warrantless search of probationer's computer was permissible given reasonable suspicion that probationer was using the computer to access the internet, in violation of the terms of his probation). There is no reported North Carolina appellate case on point.

- Authority to subject probationers to a more expansive warrantless search condition. Some judges may want to impose a warrantless search condition that is broader than the one set forth in G.S. 15A-1343(b)(13), under the catchall provision in G.S. 15A-1343(b1)(10). For example, a judge might wish to add language making it perfectly clear that the defendant must submit to searches of his computers or electronic devices, or might wish to authorize searches of such devices even if they are not in the defendant's residence, in his vehicle, or on his person. At least if the condition fashioned by the court is reasonably related to the defendant's offense and his rehabilitative needs, this is likely permissible. Courts in other jurisdictions have upheld conditions

such as suspicionless searches, see, e.g., United States v. Holm, 326 F.3d 872 (7th Cir. 2003) (finding "entirely reasonable" a condition authorizing "random searches of [a child pornography defendant's] computer"), and in some cases, the installation of software to enable continuous monitoring of the probationer's computer usage, compare United States v. Goddard, 537 F.3d 1087 (9th Cir. 2008) (upholding monitoring condition for child pornography defendant), with United States v. Sales, 476 F.3d 732 (9th Cir.2007) (rejecting broad monitoring provision for counterfeiting defendant, and stating that "[a] computer monitoring condition in some form may be reasonable. However, to comply with the Fourth Amendment, it must be narrowly tailored – producing no greater deprivation of liberty than is reasonably necessary.")

- Sex offenders. Under G.S. 15A-1343(b2)(9), sex offenders who are placed on probation must be subject to a warrantless search condition. The statute clarifies that "warrantless searches of the probationer's computer or other electronic [devices] . . . shall be considered reasonably related to the probation supervision."

C. INVENTORY SEARCHES

Warrantless inventory searches may be conducted in order to protect the owner's property while it is in police custody, protect the police against claims of lost or stolen property, and protect the police from danger. Colorado v. Bertine, 479 U.S. 367 (1987). Inventory searches must be conducted pursuant to standardized procedures. Florida v. Wells, 495 U.S. 1 (1990). The few courts to have considered the issue have mostly rejected purported "inventory" searches that extend to the contents of electronic devices. See, e.g., United States v. Davis, 2011 WL 1337372 (D. Or. Apr. 7, 2011) (citing Wall, infra); United States v. Wall, 2008 WL 5381412 (S.D. Fla. Dec. 22, 2008) ("[T]here is no need to document the phone numbers, photos, text messages, or other data stored in the memory of a cell phone to properly inventory the person's possessions because the threat of theft concerns the cell phone itself, not the electronic information stored on it."); United States v. Flores, 122 F.Supp.2d 491 (S.D.N.Y. 2000) ("[N]either a calendar book nor a cellular telephone is a 'container' that has 'contents' that need to be inventoried for safekeeping in the traditional sense of those terms.").

D. INDEPENDENT SOURCE/INEVITABLE DISCOVERY

The independent source and inevitable discovery doctrines are exceptions to the exclusionary rule, not, technically, types of warrantless search. Nonetheless, they bear mention, because some warrantless searches that are not legally permitted may nonetheless yield results that are not subject to exclusion. For example, in United States v. Hughes, __ F.3d __, 2011 WL 1332061 (1st Cir. 2011), the First Circuit considered a consent search of the defendant's computers. The defendant claimed that his consent was coerced, but the court determined that even if it was, the contents of the computers would inevitably have been discovered by search warrant, because the officers had probable cause, "had support staff on stand-by, ready to apply for a warrant, and the warrant issued the next day. That was sufficient for the inevitable discovery doctrine to take hold." Simlarly, in United States v. Stabile, 633 F.3d 219 (3rd Cir. 2011), the court considered the actions of an officer who was searching the defendant's hard disk, pursuant to a warrant, for evidence of financial crimes. The officer saw lurid file names, then viewed the files, which contained child pornography. The court applied the independent source doctrine to admit the child pornography, concluding that even if the officer exceeded the scope of the first search warrant by viewing the files, he would have sought a second warrant based on the file names, which he clearly had a right to

view under the first warrant. (It also applied the inevitable discovery doctrine to different evidence.) The related concept of plain view is discussed in my manuscript on warrant searches, so I won't repeat that discussion here.