

Electronic Evidence and the Constitution: How the Fourth Amendment Applies to Information Stored On Computers and Other Electronic Data Devices

By Brian Bernel (Part 1) and Jonah Morningstar (Part 2)

Part 1:

I. Introduction:

A laptop and its storage devices have the potential to contain vast amounts of information. People keep all types of personal information on computers, including diaries, personal letters, medical information, photos, and financial records. Attorneys' computers may contain confidential client information. Reporters' computers may contain information about confidential sources or story leads. Inventors' and corporate executives' computers may contain trade secrets. *United States v. Arnold*, 454 F. Supp. 2d. 999, 1003-4 (C.D. Cal. 2006). This paper is a general examination of the Fourth Amendment of the United States Constitution in the context of new technologies which have vastly changed the embodiment and mobility of private, and often incriminating, information.

II. Historical Background:

The Fourth Amendment of the United States Constitution protects U.S. citizens from unreasonable and warrantless searches by the government. The Fourth Amendment states:

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

U.S. Const. Amend. IV. Unchanged since its adoption in 1791, specific language of the Fourth Amendment derives from a time when privacy concerns were understood in terms of distinct, identifiable places wherein tangible things could be protected by hiding them out of sight and/or under lock and key. Since then, privacy landscape has changed considerably driven largely by continued advances in technology. Paper correspondence has been replaced by the convenience of Instant Messaging (IM), Short Message Service (SMS) texting, and e-mail. Pay phones have been supplanted by mobile phones that not only make phone calls, but can also play music, take pictures, record digital video, surf the Internet, and use telemetry from Global Positioning System (GPS) satellites to provide driving directions. In response to technological advances, the Supreme Court of the United States has interpreted and reinterpreted the text of the Fourth Amendment as new technologies become commonplace and societal norms regarding privacy evolve.

Earlier interpretation of the Fourth Amendment reflected a more literal approach tied to common law trespass. For instance, in *Olmstead v. United States*, the government secretly monitored the telephone conversations of the defendant by inserting wiretaps on the telephone lines near his home. 277 U.S. 438, 457 (1928). The Supreme Court found no Fourth Amendment protection because it interpreted such protection to extend search and seizure of

material things, and the wiretaps were installed and defendants' conversations intercepted without entry to the houses or offices of the defendants. *Id.* at 464-466.

Similarly, in a case where agents used an electronic listening device placed against the wall to record live conversations in an adjoining room, the Supreme Court again found no Fourth Amendment violation because there was no physical trespass in connection with the interception of the conversations. *Goldman v. United States*, 316 U.S. 129 (1942).

The Supreme Court subsequently relaxed its interpretation of trespass in *Silverman v. United States*. In *Silverman*, the government eavesdropped on conversations by tapping the sound carried through the heating ducts under the floorboards of a house. 365 U.S. 505, 509 (1961). The Court held that while there was an "unauthorized physical penetration," its decision did not turn upon technical trespass. *Id.* at 512. Rather, Fourth Amendment protection was implicated because there was an actual intrusion into a constitutionally protected area. *Id.*

Two years later, in *Wong Sun v. United States*, the Supreme Court specifically held that verbal evidence may be the fruit of official illegality under the Fourth Amendment along with the more common tangible fruits of unwarranted intrusion:

"The exclusionary rule has traditionally barred from trial physical, tangible materials obtained either during or as a direct result of an unlawful invasion. It follows from our holding in *Silverman v. United States*. . . that the Fourth Amendment may protect against the overhearing of verbal statements as well as against the more traditional seizure of 'papers and effects.' " 371 U.S. 471, 485, (1963).

III. Modern Interpretation:

In *Katz v. United States*, the Supreme Court formally overruled the trespass doctrine enunciated in *Olmstead* and *Goldman*, holding that physical intrusion into any given enclosure is no longer required to invoke Fourth Amendment protection. 389 U.S. 347, 353 (1967). In *Katz*, the government eavesdropped on the Katz's telephone conversations by means of an electronic listening device attached to the exterior of the phone booth from which Katz placed his calls. *Id.* at 348. The Court held the government's eavesdropping activities constituted a "search and seizure" within the meaning of the Fourth Amendment because Katz justifiably relied on the privacy of the telephone booth when he closed the door and paid to place his calls. In its decision, the Court pointed out that the focus of the arguments by both sides on whether a telephone booth is a 'constitutionally protected area' was misguided because the Fourth Amendment protects people, not places. *Id.* at 351. Thus, the fact that there was no physical intrusion because the listening device did not penetrate the wall of the booth was of no constitutional significance. *Id.* at 353. In practice, *Katz* is more often cited for Justice Harlan's concurring opinion, in which he articulated a two-part test for determining Fourth Amendment violations: (1) Whether the individual's conduct reflects an actual, subjective expectation of privacy, and; (2) whether the individual's subjective expectation of privacy is one that society is prepared to recognize as reasonable. *Id.* at 361.

The Court subsequently applied the principles from *Katz* in determining that a number of other government activities did not constitute searches under the Fourth Amendment. *Smith v. Maryland*, 442 U.S. 735, 743-744 (1979) (holding that it is not a search for the police to use a pen register at the phone company to determine what numbers were dialed in a private home). *Dow Chemical Co. v. United States*, 476 U.S. 227, 237 (1986) (holding that enhanced aerial photography of an industrial complex is not a search implicating privacy concerns under the

Fourth Amendment). *Florida v. Riley*, 488 U.S. 445 (1989) (holding that naked-eye aerial surveillance of a private home and surrounding area does not constitute a search). In *California v. Ciraolo* the Court held that a Fourth Amendment search does not occur, even when the protected location of a house is concerned, unless the individual manifests a subjective expectation of privacy in the object of the challenged search and society is willing to recognize that expectation as reasonable. 476 U.S. 207, 210 (1986). More recently, the Supreme Court grappled with applying the principles from *Katz* and *Ciraolo* to the government's use of emergent technologies to gather evidence during an investigation. In the course of a narcotics investigation, government agents used a thermal imager to detect anomalous heat signatures on the outside of a defendant's home which the agents believed were consistent with the use of high-intensity lamps used to grow marijuana inside the defendant's home. *Kyllo v. United States*, 533 U.S. 27 (2001). In his opinion for the majority, Justice Scalia ruled that the government's use of sense-enhancing technology not otherwise in general public use to gather information on the interior of a home that could not otherwise be obtained without physical intrusion constitutes an impermissible search under the Fourth Amendment. *Id.* at 34-35. A potential problem with this holding, which is also raised in Justice Kennedy's dissent, is that the qualifier, "not in general public use," fails to adequately address what is perhaps the main issue inherent to emergent technologies and privacy; that is, what amount of use certifies a new technology as being "in general public use," and what happens to privacy issues once the use of technology initially deemed "intrusive" becomes commonplace? *Id.* at 47.

IV. Reasonable Expectation of Privacy:

As a starting point, the prohibition against unreasonable searches and seizures contained in the Fourth Amendment ordinarily applies only to governmental agencies and not to private persons, so long as the private party is not acting as an agent of the government or with the participation of any government official. *United States v. Jacobson*, 466 U.S. 109, 133 (1984).

Information kept in a closed container is entitled to Fourth Amendment protection. *United States v. Ross*, 456 U.S. 798, 822-23 (1982). Courts generally compare information stored in computers, pagers, and other electronic storage devices as similar, for Fourth Amendment purposes, to items in a closed container and therefore subject to the same reasonable expectation of privacy. *United States v. Barth*, 26 F. Supp. 2d. 929, 936-37 (W.D. Tex. 1998) (defendant had reasonable expectation of privacy regarding information stored on a computer hard drive); *United States v. Blas*, 1990 WL 265179 (E.D. Wis. 1990) ("an individual has the same expectation of privacy in a pager, computer, or other electronic data storage and retrieval device as in a closed container").

There is less consensus, however, on the autonomy of individual files and directories as closed-containers stored on a device. For example, the Fifth Circuit in *United States v. Runyan* found that a disk drive containing multiple files is a single closed container for Fourth Amendment purposes. 275 F.3d 449, 464-65 (5th Cir. 2001). Whereas in *United States v. Carey*, the Tenth Circuit found that the scope of warrant authorizing a search for drug-related information on defendant's hard drive did not extend to a search of image files for child pornography. 172 F.3d 1268 (10th Cir. 1999). Not surprisingly, the Fourth Amendment particularity requirement for warrants is often implicated where courts appear to disagree.

In order to properly conduct a search or seizure of computer equipment under the auspices of a warrant, the warrant must meet the particularity requirement of the Fourth

Amendment and be supported by probable cause.¹ There are two distinct components to the particularity requirement. First, the warrant must describe the things to be seized with sufficient precision such that it tells the officers how to differentiate items properly subject to seizure from irrelevant items. *Davis v. Gracey*, 111 F.3d 1472, 1478 (10th Cir. 1997). Second, the description of things to be seized must not be overbroad that it encompasses items that should not be seized. *Id.* There are a number of cases where courts have come to different conclusions on similar sounding language in warrants calculated to recover evidence stored on a computer and any attached or related data storage devices. For example, in *United States v. Hersch*, the court found that a warrant permitting the seizure of all computer hardware, software, and related equipment did not violate the particularity requirement of the Fourth Amendment. 1994 WL 568728 (D. Mass. 1994). Whereas the court in *United States v. Hunter*, held that a search warrant which called for seizure of all computers, all computer storage devices, and all computer software systems was a catch-all warrant lacking sufficient limitation, so that the warrant was overbroad and failed to comply with the Fourth Amendment particularity requirement. 13 F. Supp. 2d 574 (D. Vt. 1998).²

In certain circumstances an individual can abrogate their reasonable expectation of privacy in information stored on a computer. An individual has no reasonable expectation of privacy in information that appears on the computer screen and of which individual is aware to be visible to bystanders. *United States v. David*, 756 F. Supp. 1385, 1389 (D. Nev. 1991). Nor does an individual have a reasonable expectation of privacy in the information on a computer they have stolen. *United States v. Lyons*, 992 F.2d 1029, 1031-32 (10th Cir.1993); *see also United States v. Caymen*, 404 F.3d 1196 (9th Cir. 2005) (holding defendant had no legitimate expectation of privacy in contents of hard drive of computer that he obtained by fraud, and thus lacked Fourth Amendment standing to challenge a search of the hard drive by police). The reasonable expectation of privacy can also be lost where the searched information resides on the computer of a third-party after being sent to the third-party via e-mail, because the originator no longer has a reasonable expectation of control over the information. *United States v. Horowitz*, 806 F.2d 1222 (4th. Cir. 1986). For the same reason, the reasonable expectation of privacy is lost in information e-mailed to a computer bulletin board, *e.g. Guest v. Leis*, 255 F.3d 325 (6th Cir. 2001), and or disclosed in internet chat-room conversations, *e.g. United States v. Charbonneau*, 979 F. Supp. 1177 (S.D. Ohio 1997). To the extent that the originator may initially retain a right to control a third-party's possession, the general rule is that the originator's Fourth Amendment rights dissipate as the sender's right to control the third-party's possession

¹ The Supreme Court modified the Fourth Amendment exclusionary rule in *United States v. Leon*, so as not to bar the use, in the prosecution's case in chief, of evidence obtained by officers acting in reasonable reliance on a search warrant issued by a detached and neutral magistrate which ultimately is found to be defective. 468 U.S. 897, 104 S.Ct. 3405, 82 L. Ed.2d 677 (1984). This is sometimes called the "Good Faith Exemption."

² This disparity may have less to do with disagreements between courts on the legal efficacy of specific words in "what and where" warrant language than the result of weak specificity accompanied by vague probable cause. *Cf. United States v. Clough*, 246 F. Supp. 2d. 84 (D. Me. 2003) (scope of search warrant authorizing seizure of any text documents or digital images on defendant's computers was excessive because it contained no restrictions on search, no references to statutes, and no references to crimes or illegality); *Cf. United States v. Riccardi*, 405 F.3d 852 (10th. Cir. 2005) (warrant to seize and examine defendant's computer which was not limited to any particular files, or to any particular federal crime, failed to satisfy Fourth Amendment's particularity requirement); *Cf. United States v. Summage*, 425 F. Supp. 2d 995 (S.D. Iowa 2006) (warrant allowing for seizure of digital video recording devices and equipment lacked sufficient particularity to limit executing officers' search, where there were no specific crimes alleged against defendant which would have limited the search).

diminishes. *See United States v. Poulsen*, 41 F.3d 1330 (9th Cir. 1994) (Introduction at trial of defendant's computer tapes which were recovered from a commercial locker by the government during a warrantless search does not violate defendant's reasonable expectation of privacy because his right to access the tapes ended when he neglected to pay the required locker rental fee).

V. Exceptions to the Fourth Amendment Warrant Requirement:

There are a number of exceptions to the warrant requirement that are relevant to computer searches; (1) direct consent, (2) implied consent³, (3) third-party consent, including spouses/domestic partners, parents, and system administrators⁴, (4) special needs, (5) exigent circumstances, (6) "plain view," (7) searches incident to a lawful arrest, and (8) border searches. Only third-party consent and border searches will be covered here, as they are the most pertinent to computer searches.

Third-party consent is applicable when the computer equipment (or electronic storage device) is used or owned by several people. One who has common authority over premises or effects may consent to a search even if an absent co-user objects. *United States v. Matlock*, 415 U.S. 164, 171 (1974). Therefore, all users of the computer assume the risk that a co-user might discover the data of other users and subsequently permit law enforcement to search this "common area" as well. However, the search should be limited to the zone of the consenting co-user's common authority. *United States v. Jacobsen*, 466 U.S. 109, 119 (1984). This means that the government must determine the scope of the co-user's access and clarify boundaries of common authority under which the co-user can validly consent to a search. *United States v. Blok*, 590 F.2d 535, 542 (4th Cir. 1987). For example, when a user password-protects her files and does not share the passwords with other co-users of the computer, then the protected files are excluded from the scope of consent that can be validly granted by the co-users. *Trulock v. Freeh*, 275 F.3d 391, 403-04 (4th Cir. 2001).

In a family context, absent an affirmative showing that a consenting spouse lacks access to a particular searched property, an individual's spouse may validly consent to a search of all the couple's property. *United States v. Duran*, 957 F.2d 499, 504-05 (7th Cir. 1992). Parental consent to a search of their children's room is generally valid where the child is a minor. However, courts are unlikely recognize parental consent to a child's room or private areas where the child is not a minor, pays rent, and/or denies access to the parents. *See United States v. Whitfield*, 939 F.2d 1071, 1075 (D.C. Cir. 1991).

As mentioned in the footnote, third-party consent given by system administrators is usually governed by the ECPA. However, if the individual's computer is attached to a network of a state institution (and thus the system administrator is an employee of the state), then the special needs exception may apply. Most recently, in *United States v. Heckencamp*, the Ninth Circuit held that while a student at a state university retained an objectively reasonable expectation of privacy on his computer after it was attached to the university network, a remote

³ For the purpose of brevity, direct and implied consent are not covered in this paper.

⁴ While there are constitutional implications to consent given by a system administrator, in practice, system administrators are considered agents of "provider[s] of electronic communication service" under the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2701-2712, which regulates law enforcement efforts to obtain consent from system administrators to search an individual's account.

search of the student's computer by the university network administrator was justified under the special needs exception because administrator acted to protect the network security and not to collect evidence for law enforcement after discovering that the student had gained unauthorized root access to the server. 482 F.3d 1142 (9th Cir. 2007), *cert. denied*, 2007 WL 3021387 (U.S. 2007).

The government can also conduct warrantless searches under "exigent circumstances," i.e. in circumstances that "would cause a reasonable person to believe that entry . . . was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts." See *United States v. McConney*, 728 F.2d 1195, 1199 (9th Cir. 1984) (en banc). For example, if government agents see a suspect attempting to delete files from his computer the agents can seize the computer to prevent destruction of evidence. See *United States v. David*, 756 F. Supp. 1385, 1392 (D.Nev 1991). On the other hand, the exigency ends once the agents have seized the computer and a search of the stored data would still likely require a warrant. *Id.*

Under the plain view exception, evidence can be seized without a warrant so long as seizing agent is in a lawful position to observe and access the evidence, and the incriminating character of the evidence is immediately apparent. See *Horton v. California*, 496 U.S. 128 (1990). It is important to remember that this exception only applies to seizure, and the reasonable expectation of privacy still imposes limits on warrantless searches in this context.

Perhaps the most common exception to warrant requirement is where a warrantless search is conducted incident to a lawful arrest. This is a limited exception which places temporal and spatial limitations on searches incident to arrest, excusing compliance with the warrant requirement only when the search is substantially contemporaneous with, and confined to immediate vicinity of the arrest. *Holmes v. Kucynda*, 321 F.3d 1069 (11th Cir. 2003). Moreover, the search conduct must be reasonable in light of the facts and circumstances at the time of the arrest. *Wyatt v. Slagle*, 240 F. Supp. 2d. 931 (S.D. Iowa 2002); *Graham v. Connor*, 490 U.S. 386, 396-97 (1989). Courts have found searches of traditional "analog data containers" such as wallets, purses, or briefcases to fall under this exception. See *United States v. Castro*, 596 F.2d 674, 676 (5th Cir. 1979) (holding that agents may inspect the entire contents of a suspect's wallet found on his person); *United States v. Syler*, 430 F.2d 68 (7th Cir. 1970) (holding that a search of the defendant's purse found in her room after she was arrested at her home was reasonable as a search incident to a lawful arrest); *United States v. Johnson*, 846 F.2d 279, 283-84 (5th Cir. 1988) (holding that search of a defendant's briefcase that was at his side at the time of arrest was permissible). In terms of its applicability to "digital" storage mediums, courts have found viewing the numbers stored on a suspect's electronic pager within twenty minutes of his arrest to be permissible. See *United States v. Reyes*, 922 F. Supp. 818, 833 (S.D.N.Y. 1996). Similarly, some courts have found that traditional warrant exceptions apply to the search of data stored on cell phones. See e.g. *United States v. Parada*, 289 F. Supp 2d. 1291, 1304 (D. Kan. 2003) (finding officer's accessing the memory of a suspect's cell phone to view stored numbers of incoming calls was justified by exigency); *United States v. Finley*, 477 F.3d 250, (5th Cir. 2007) (upholding retrieval of call records and text messages from cell phone as search incident to arrest). Yet, while a pager is certainly a type of electronic data storage device, it is still extremely primitive with respect to complexity and data storage in comparison to storage capacity and multimedia capabilities of modern-day mobile phones. It is not yet clear whether warrantless searches that capture other types of mobile phone data, such as digital

sound/video recordings, digital photographs, and other types of stored data beyond phone numbers and SMS texts will affect the courts' analysis. Considering the technical steps/expertise necessary (and the increased execution time associated with those steps) to conduct a search of data stored on a computer, as well as the divergence in court holdings on the validity of these searches under the plain view doctrine, the incident to a lawful arrest exception is unlikely to become of much use to law enforcement outside the context of mobile phones and pagers.

Finally, routine searches at the borders of the United States do not require a warrant, probable cause, or even reasonable suspicion that contraband or other evidence will be discovered as a result. *United States v. Montoya De Hernandez*, 473 U.S. 531, 538 (1985). The Supreme Court recognized this special exception in order to protect the government's ability to prevent contraband and other property from entering United States illegally, as well for regulating the collection of duties. *Id.* at 537. The balance is struck more favorably toward the government because of the lessened expectation of privacy and the need to protect the nation's borders. *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004). As a result of the heightened need of the government, the examination of items such as luggage, purses, wallets, and pockets is considered "routine" and requires no suspicion. *Montoya De Hernandez*, 473 U.S. at 538. However, some searches are so intrusive that they require particularized suspicion to be reasonable. *United States v. Guadalupe-Garza*, 421 F.2d 876, 879 (9th Cir. 1970). The reasonableness of a border search is determined by balancing the need for a particular search against the invasion that the search entails. *Id.* at 878. Highly intrusive searches can implicate the "dignity and privacy interests of the persons being searched." *Flores-Montano*, 541 U.S. at 152. In *United States v. Arnold*, the court granted the defendant's motion to suppress evidence of child pornography recovered during a border search of the defendant's laptop hard drive, CD-ROMs, and flash-memory storage media. 454 F. Supp. 2d 999, 1000-1001 (C.D. Cal. 2006)⁵. The court held that opening and viewing confidential computer files constituted a non-routine and invasive border search that implicated privacy and dignity. *Id.* at 1003. Thus, because the government failed to carry its burden of a reasonable suspicion, customs agents' search violated the Fourth Amendment. *Id.* at 1006.

Fourth Amendment application to searches of computers in the workplace differ depending on whether the search takes place in the public or private sector. The standards for conducting private-sector searches is generally the same as those for searches in homes and personal residences. Thus, private sector workers generally retain a reasonable expectation of privacy in their office space unless that space is "open to the world at large." *United States v. Lyons*, 706 U.S. 706 F.2d 321, 326 (D.C. Cir. 1983). Similarly, use of a privately-owned computer in a public sector workplace without any attempt to password-protect or prevent third-party use can negate an individual's reasonable expectation of privacy in the computer. *United States v. Barrows*, 841 F.3d 1246 (10th Cir. 2007). With respect to public sector employment, government employees can also enjoy a reasonable expectation of privacy in their work space, but this determination is done on a case-by-case basis, and the expectation can become unreasonable if actual office practices and procedures permit the employee's supervisor, co-workers, or the public to enter the employee's workspace. *O'Connor v. Ortega*, 480 U.S. 709, 717 (1987). In particular, the existence of search-authorizing notices or regulations has consistently been interpreted by the courts as negating a reasonable expectation of privacy on the part of the employee. See *American Postal Workers Union, Columbus Area Local AFL-CIO v.*

⁵ This case was argued on appeal before the Ninth Circuit on October 18, 2007. As of this writing, the Ninth Circuit has not yet decided the case.

United States Postal Service, 871 F.2d 556, 59-61 (6th Cir. 1989) (holding that postal employees retained no reasonable expectation of privacy in contents of government lockers after signing waivers stating that lockers were subject to inspection at any time). In *United States v. Simons*, the court found that a federal employee possessed a legitimate expectation of privacy in his office for Fourth Amendment purposes, where the employee did not share his office, and there was no evidence of any workplace practices, procedures, or regulations that had effect of diminishing his legitimate privacy expectations. 206 F.3d 392, 399 (4th Cir. 2000). However, the court also found that government employer's remote, warrantless search of the employee's office computer did not violate the employee's Fourth Amendment rights because, the employer's internet policy clearly stated that the employer would "audit, inspect, and/or monitor" employee's use of the Internet, including all file transfers, all websites visited, and all e-mail messages, "as deemed appropriate," which placed the employees on notice that they could not reasonably expect that their Internet activity would be private. *Id.* at 389. After *O'Connor*, government employers' intrusions on the constitutionally protected privacy interests of its employees for non-investigatory, work-related purposes, as well as for investigation of work-related conduct will be judged by a standard of reasonableness under the circumstances. *O'Connor*, 480 U.S. 709.

VI. Conclusion of Part 1:

With the development of new technologies and increased mobility of private information, the interpretation and application of the Fourth Amendment has evolved from its roots in trespass doctrine in order to address the changing societal expectations on what should reasonably be protected from search or seizure by the government. The next section of this paper addresses in more detail the interaction between privacy and new technology and discusses potential developments for the future application of the Fourth Amendment.

Part 2: Privacy and New Technology

As discussed above, *Katz v. United States*, 389 US 347 (1967), shifted the focus of the court's Fourth Amendment analysis from trespass to privacy. Justice Harlan's test from the *Katz* opinion only protects that which is both objectively and subjectively private. In *Kyllo*, the Court based its conclusion on the fact that the heat detection equipment used by the police was not a widely used technology. In contrast, aerial surveillance by police helicopters or airplanes is not a search because helicopters and airplanes are widely held, and therefore one's subjective sense of privacy in a fenced or walled yard or patio is objectively unreasonable. As technology improves, less and less areas of our lives will be private from an objective point of view, which will affect the courts' treatment of evidence gathered from improved technology. The thermal detection equipment used in *Kyllo* or night-vision goggles are examples of already developed products. However, as technology improves, it is possible that products could be developed to hear conversations through walls, as voices cause minute vibrations in the walls and windows of a room. In that future, perhaps you don't have an expectation that your nosy neighbors, police, or identity-thieving criminals are not listening to you unless you go into your vacuum-sealed soundproof "privacy den" to have those important conversations.

Before addressing whether or not the government's search violated the defendant's privacy, there is a gateway issue of non-governmental versus governmental searches to be resolved. Private searches can produce legal evidence, no matter how shockingly conducted they might be (think for example a robber turning in child pornography evidence found by stealing the defendant's computer.) Instead of focusing on the legitimacy of the search, the court instead must determine that the private actor was not acting at the direction of the government. *US v. Jacobsen*, 466 US 109 (1984). In the field of cyber-privacy, this issue can come up with computer repair or technical support professionals. When repairing a computer, a repairman may discover child pornography accidentally while repairing a computer and turn it over to the police. Or he could think a particular customer looks like a creep and use his hacking skills to break through the customer's passwords and find child porn and turn it in. Both of these scenarios would produce legal evidence. However, what about after that first time? When the tech support fellow turns in the next customer, he has already had contact with law enforcement (in turning in the first defendant.) Maybe the first detective told the tech support fellow "good work, keep your eyes open in the future." If that is the case, the second search would probably not be allowed under the exception for non-governmental searches.

The other "exception" is also something of a gateway issue, although it also does somewhat defy categorization. All of these rules are ultimately defined by the US Supreme Court and its interpretation of the US Constitution. However, in the age of terrorism, there appears to be a de-facto "terrorism exception" to the right to privacy. Governmental monitoring of otherwise private and constitutionally-protected telephone communication after the terrorist attacks of September 2001 can be explained by creating a distinction between limits on governmental anti-crime efforts and governmental anti-terrorism efforts.

Assuming that there is a governmental search of a non-terrorist, consent might allow the use of otherwise constitutionally-protected materials. This is not an exception to the right to privacy; instead, consent can be seen as the defendant evidencing his or her lack of subjective privacy. Co-owners of a home or any other property can consent on behalf of absent co-owners, even if the co-owner later objects, assuming the police believe that the co-owner has the

authority to consent. *US v. Matlock*, 415 US 164 (1974). This issue arises in the cyber-privacy context with shared computers. Any user of a shared computer can consent to a search of the computer's contents. Password protected areas are considered common areas if the co-user who is present and consenting knows the other user's password.

Similar to consent, evidence obtained through governmental use of undercover agents is considered voluntarily relinquished by the defendant and therefore not subjectively private. In general, when a defendant voluntarily talks to an undercover agent, no search has occurred. However, the undercover agent could potentially entrap the defendant into committing the crime. In *Jacobson v. US*, 503 US 540 (1992), the defendant successfully showed the two key elements of an entrapment defense. First, that government's repeated child porn related solicitations induced him into committing the crime of ordering child porn from a government-operated mail-order service. Second, the defendant showed that he had no disposition to buy illegal child porn without the government's inducement. The test used in *Jacobson* weighs the inducement and predisposition elements together; that is, when the government must use a lot of inducement on the defendant, this fact tends to evidence less predisposition in the defendant's character, and vice versa.

Distinct from the recent and broad "terrorism exception" to privacy concerns, there are also national security issues in cyber-privacy that fit within more traditional exceptions to the right to privacy. Borders and airports are considered to be places with limited objectively reasonable privacy, including the contents of any electronic equipment brought across an international border. *US v. Romm*, 455 F3d 990 (9th Cir. 2006). The government may search people in these special areas with a little or no individualized suspicion. Recently, individuals entering the United States have reported having their computers seized permanently, or having their hard drives mirrored, or being forced to enter their encryption passwords for customs officials. While the government's "cyber border security" is still nascent, customs officials may in the future create more extensive protocols for protecting the border from electronic contraband, and for collecting electronic evidence from suspicious individuals. Furthermore, the military and intelligence agencies of the US government already have information warfare units, for the purpose of protecting secret information and technology critical for almost all military and intelligence functions.