**FSCS 620 Legal: Digital Search & Seizure Mini Assessment**

1. **A defendant's live-in girlfriend found child pornography on his computer. While the girlfriend went on a shopping trip with the defendant, she had a friend go to their house and enter it and download the child porn onto discs and take them to the police. Do the girlfriend's actions raise any 4th amendment issues? Why or why not?**

**Answer:** In the scenario where the defendant's live-in girlfriend discovered child pornography on his computer and had a friend enter their house to download the content onto discs and deliver them to the police, this situation generally does **not raise any 4th Amendment issues**. Here's why:

- The **Fourth Amendment** applies only to **governmental actions** and is intended to protect individuals from **unreasonable searches and seizures** conducted by **government actors**, such as police officers. However, when a **private individual**, acting independently and not as an agent of the government, conducts a search, the Fourth Amendment does not apply. This principle is based on the **private search doctrine**, as established in cases like **United States v. Jacobsen (1984)**, which held that "the Fourth Amendment is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government."
- In this case, both the girlfriend and her friend are **private individuals** who acted independently, without any prior **involvement or direction from law enforcement**. This makes it a **private search**, which the Fourth Amendment does not cover. Since there was no **government instigation**, participation, or knowledge of their actions beforehand, the search and collection of evidence would not raise Fourth Amendment concerns.
- Furthermore, under **United States v. Jacobsen (1984)**, once the results of a **private search** are brought to law enforcement, the police may act on the evidence **without a warrant**, as long as they do not **exceed the scope** of the original private search.
- Therefore, based on these precedents, the actions of the girlfriend and her friend are considered lawful under the **private search doctrine** and do not raise Fourth Amendment concerns.
- **Fourth Amendment and State Action**: It is essential to note that **Fourth Amendment protections only apply to actions by the government** or its agents. In this case, since the girlfriend and her friend acted as **private individuals** and were not directed by law enforcement, their actions are not constrained by the Fourth Amendment. This principle is well-established in **Burdeau v. McDowell (1921)**, where the Court ruled that **the Fourth Amendment does not apply to searches or seizures conducted by private individuals without government involvement**.
- It is important to note that once a private individual hands over evidence to law enforcement, any subsequent search by the police must remain within the **scope of the original private search**. In other words, law enforcement officers may act on the evidence obtained through the private search without a warrant, but they cannot exceed the scope of what was initially discovered by the private individual without obtaining a valid search warrant.

## Key Laws and Precedents:

1. **United States v. Jacobsen (1984)**:
   - The Supreme Court held that **"the Fourth Amendment is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government."**
   - This case establishes that **private searches** do not violate Fourth Amendment rights unless the private individual was acting at the **direction of law enforcement**.
2. **Walter v. United States (1980)**:
   - Reinforces that private individuals acting on their own initiative do not trigger Fourth Amendment protections.
3. **Burdeau v. McDowell (1921)**:
   - The Fourth Amendment applies only to government actions, and private searches are not covered unless the individual is acting as a government agent.

## Conclusion:

The actions of the girlfriend and her friend do not raise Fourth Amendment issues because they acted independently, without government direction, falling under the **Private Search Doctrine** established by **United States v. Jacobsen (1984)**. Consequently, their actions would not violate the defendant's Fourth Amendment rights.

**2. A defendant kidnapped a bank vice president and sent a ransom note for money in exchange for her safe return, but ended up killing her, anyway. The FBI executing a search warrant for the contents of his computer found the ransom note in it. He had deleted it from his directory, but the officers used a program designed to find deleted files. The defendant argued that an additional search warrant should have been obtained to use this deleted file recovery program. Are there any 4th amendment issues here? Why or why not?**

**Answer:** In the scenario where the FBI executed a valid search warrant on the defendant's computer and used a program to recover deleted files, including the ransom note, there are **no Fourth Amendment issues** raised. Here's why:

- **Scope of the Warrant**: The **Fourth Amendment** requires that a search warrant be specific in describing the place to be searched and the items to be seized. The FBI's original warrant would have authorized the search of the defendant's computer for evidence related to the crime, such as the ransom note. **Deleted files** are still considered part of the computer's contents, and courts have held that law enforcement can use **forensic tools** to recover deleted data without needing an additional warrant. This principle was established in **United States v. Grimmett (2006)**, where the court held that "a computer search may be as extensive as reasonably required to locate the items described in the warrant."
- **Forensic Techniques**: The **Fourth Amendment** does not limit the methods law enforcement can use, as long as they remain within the scope of the warrant. In this case, the FBI's use of a **program to recover deleted files** was permissible because the search warrant authorized a thorough examination of the computer's contents, including the use of specialized forensic tools. As long as the search remains focused on finding evidence related to the crime, the use of such techniques is lawful. This is confirmed in **United States v. Long (2005)**, which held that the use of forensic software to search a computer's data does not violate the Fourth Amendment, provided the search stays within the scope of the warrant.

- **No Expectation of Privacy in Deleted Files**: Once a valid warrant is obtained, law enforcement can recover **deleted files** without needing a separate warrant. Deleted files are still part of the computer's contents, and their recovery is lawful if it falls under the scope of the warrant. In **United States v. Upham (1999)**, the court ruled that the recovery of deleted files during a valid search is lawful and does not require an additional warrant.
- The key legal principle here is that law enforcement must ensure that the search does not **exceed the scope** of the original warrant. The recovery of deleted files is considered part of the computer's contents, but the search must remain focused on finding evidence directly related to the crime as authorized by the warrant. If law enforcement had expanded the search beyond the areas specified in the warrant, it could have raised Fourth Amendment issues.
- **Fourth Amendment's "Particularity Requirement"**: The **Fourth Amendment** requires that warrants must describe **with particularity** the places to be searched and the items to be seized. In this case, the warrant specifically authorized the search of the defendant's computer for evidence related to the crime, including the recovery of deleted files. This is consistent with the **"particularity requirement"** under the Fourth Amendment, which ensures that searches are not overly broad. In **Marron v. United States (1927)**, the Court emphasized the importance of warrants being sufficiently specific in describing the items to be seized.

## Relevant Laws and Case Precedents:

1. **United States v. Grimmett (2006)**:
    - The court held that a search warrant for a computer may extend to all areas where the items described in the warrant could reasonably be found, including deleted files. This ruling confirms that recovering deleted files falls within the scope of the search warrant.
2. **United States v. Long (2005)**:
    - This case supports the use of forensic tools to examine data on a computer during a search. The Fourth Amendment does not limit the specific techniques law enforcement may use, as long as they are within the bounds of the warrant.
3. **United States v. Upham (1999)**:
    - The court ruled that law enforcement can recover deleted files during a search and does not need an additional warrant to do so. The recovery of deleted files is lawful if covered under the original search warrant.
4. **Marron v. United States (1927)**:
    - The Court established the **"particularity requirement"**, which requires warrants to specifically describe the scope of the search to prevent overly broad searches.

## Conclusion:

There are **no Fourth Amendment issues** in this case because the search warrant authorized the search of the defendant's computer, including the recovery of deleted files. The FBI's use of forensic software to recover deleted files was within the scope of the warrant, and **no additional warrant** was necessary. The case law, including **United States v. Grimmett** and **United States v. Upham**, supports the use of forensic tools during a valid search without violating the Fourth Amendment.

3. **A US citizen female traveler just arrived alone to Baltimore Airport from Cairo Egypt. The traveler approaches a US Customs and Border Patrol agent to gain entry into the USA. The CBP officer asks the traveler for her passport and where she is flying in from. The CBP officer also asks the traveler to turn on her cell phone and show him her contact list. Is a search warrant required before the CBP officer can access the cell phone? Why or why not. Please use at least ten sentences to answer this question and justify your response.**

**Answer:** In the context of border searches, such as the scenario described, **no search warrant is required** for the Customs and Border Protection (CBP) officer to access the traveler's cell phone at the U.S. border. This is due to the **"border search exception"** to the Fourth Amendment, which allows routine searches at U.S. borders without a warrant, probable cause, or reasonable suspicion. Here's a detailed analysis:

- **Fourth Amendment at the Border**: The Fourth Amendment protects individuals against unreasonable searches and seizures. However, the U.S. Supreme Court has long recognized an exception for searches at the border, where the government's interest in protecting the country justifies a relaxation of typical Fourth Amendment requirements.
- **Border Search Exception**: According to the case **United States v. Montoya de Hernandez (1985)**, routine searches at the border do not require a warrant or probable cause. The Court ruled that the government's interest in national security and preventing contraband from entering the country overrides the individual's expectation of privacy at the border.
- **Electronic Devices**: The courts have extended this exception to include searches of electronic devices, such as cell phones. In **United States v. Arnold (2008)**, the Ninth Circuit ruled that reasonable suspicion was not necessary for customs officers to search a laptop or other electronic storage devices at the border. This ruling has been interpreted to apply to cell phones as well.
- **Routine vs. Non-Routine Searches**: While routine searches at the border do not require any suspicion, more invasive searches (such as searches involving destruction or extreme invasion of privacy) may require some level of suspicion. However, in this case, simply requesting access to a contact list on the traveler's phone would likely be considered routine.
- **Balancing Privacy and Security**: The courts have emphasized that the government's interest in preventing illegal activities, such as smuggling and terrorism, outweighs the privacy rights of individuals crossing the border. This rationale was reinforced in **United States v. Flores-Montano (2004)**, which stated that the government's authority to search at the border is at its peak when protecting the country's sovereignty.
- **Supreme Court Precedent**: The Supreme Court has held that **privacy expectations are diminished** at the border. The **Riley v. California (2014)** decision, which required a warrant for cell phone searches during an arrest, does not apply to border searches because they are governed by a different legal standard, as seen in **United States v. Cotterman (2013)**, where a warrantless forensic search of a laptop was upheld at the border.
- **Statutory Authority**: Under **19 U.S.C. § 1581**, customs officers are authorized to search any person, luggage, or merchandise crossing the U.S. border without a warrant.
- **No Warrant Requirement**: Therefore, based on the **border search exception** and established case law, a search warrant is not required for the CBP officer to inspect the traveler's cell phone and contact list upon her entry into the United States.

- However, it is also important to understand that **non-routine searches** at the border, such as forensic analysis of electronic devices or invasive searches, may require **reasonable suspicion**. Courts have distinguished between routine and non-routine searches, with the latter requiring a higher threshold. In this case, the request to view a contact list would likely be considered a **routine search** that does not require suspicion or a warrant.

In conclusion, the CBP officer's actions in this scenario are lawful under the **border search exception** to the Fourth Amendment, and no additional warrant is necessary to access the phone's contents during the routine inspection.

**Relevant Laws and Case Precedents:**

1. **United States v. Montoya de Hernandez (1985)**:
    - The Supreme Court ruled that **routine border searches** do not require a warrant or probable cause. The government's interest in national security justifies a relaxation of Fourth Amendment protections at the border.
2. **United States v. Arnold (2008)**:
    - The Ninth Circuit held that **electronic devices**, such as laptops and cell phones, may be searched at the border without reasonable suspicion or a warrant under the border search exception.
3. **United States v. Flores-Montano (2004)**:
    - Reinforced that the government's **authority to conduct searches at the border** is broad and does not require suspicion for routine searches.
4. **United States v. Cotterman (2013)**:
    - The Ninth Circuit allowed a **forensic search** of a laptop at the border, reaffirming that more invasive searches may require reasonable suspicion, but routine searches remain permissible without any suspicion.
5. **United States v. Ramsey (1977)**:
    - Established that the **border search exception** allows for warrantless searches due to the government's need to protect national security, emphasizing the **reduced expectation of privacy** at the border.
6. **19 U.S.C. § 1581**:
    - This statute gives **Customs and Border Protection (CBP)** the authority to conduct searches of any person, luggage, or merchandise crossing the border without a warrant.

**References:**

DOJ Electronic Law and Evidence pdf from canvas
Electronic Evidence pdf from canvas
https://constitution.congress.gov/browse/amendment-4/#:~:text=The%20right%20of%20the%20people,and%20the%20persons%20or%20things