Criminal Procedure: Comprehensive Guide

Main Sections:

Note: This guide provides a systematic approach to evaluating key doctrines in Criminal Procedure, with a focus on Professor Sood's course. Each section includes detailed flowcharts with specific criteria for applying the constitutional standards along with key cases.

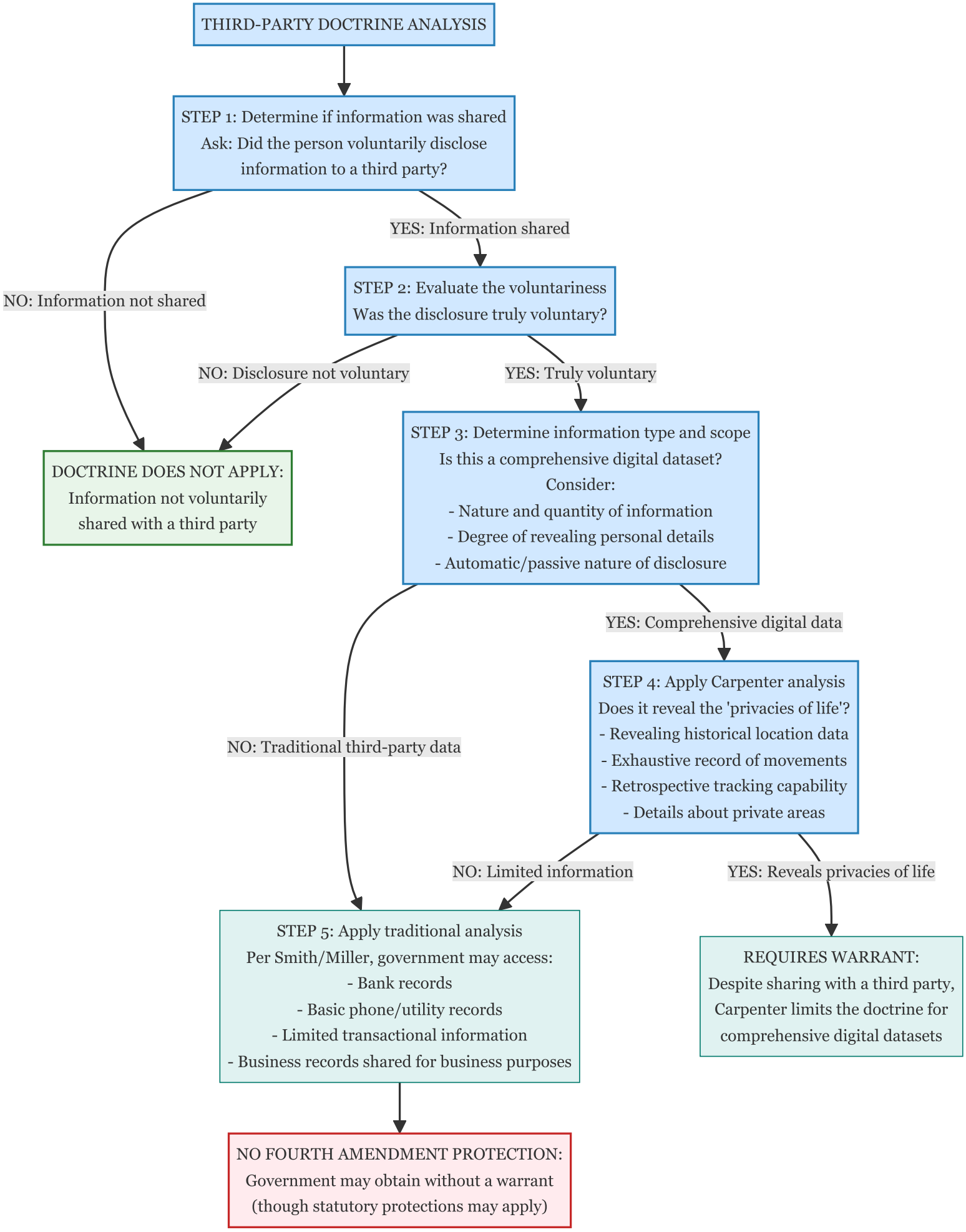
Third-Party Doctrine

The Third-Party Doctrine Explained

The third-party doctrine holds that information voluntarily disclosed to third parties generally receives no Fourth Amendment protection. Under this principle, when a person shares information with a third party, they assume the risk that the third party may provide that information to the government.

Core Principles of the Third-Party Doctrine

- **Voluntary Disclosure**: When someone voluntarily shares information with a third party, they assume the risk of further disclosure
- **No Reasonable Expectation of Privacy**: A person typically has no reasonable expectation of privacy in information shared with others
- **No Fourth Amendment Protection**: Without a reasonable expectation of privacy, obtaining the information is not a "search" requiring a warrant
- **Information vs. Content**: Traditionally distinguishes between transactional records (less protected) and communications content (more protected)
- **Evolving Doctrine**: Recent cases have limited the doctrine's scope in the digital age


THIRD-PARTY DOCTRINE ANALYSIS
STEP 1: Determine if information was shared
Ask: Did the person voluntarily disclose information to a third party?
NO: Information not shared
YES: Information shared
STEP 2: Evaluate the voluntariness
Was the disclosure truly voluntary?
NO: Disclosure not voluntary
YES: Truly voluntary
DOCTRINE DOES NOT APPLY:
Information not voluntarily shared with a third party
STEP 3: Determine information type and scope
Is this a comprehensive digital dataset?
Consider:
- Nature and quantity of information
- Degree of revealing personal details
- Automatic/passive nature of disclosure
NO: Traditional third-party data
YES: Comprehensive digital data
STEP 4: Apply Carpenter analysis
Does it reveal the 'privacies of life'?
- Revealing historical location data
- Exhaustive record of movements
- Retrospective tracking capability
- Details about private areas
NO: Limited information
YES: Reveals privacies of life
STEP 5: Apply traditional analysis
Per Smith/Miller, government may access:
- Bank records
- Basic phone/utility records
- Limited transactional information
- Business records shared for business purposes
REQUIRES WARRANT:
Despite sharing with a third party, Carpenter limits the doctrine for comprehensive digital datasets
NO FOURTH AMENDMENT PROTECTION:
Government may obtain without a warrant (though statutory protections may apply)

United States v. Miller *425 U.S. 435 (1976)*

A bank depositor has no legitimate expectation of privacy in financial information voluntarily conveyed to banks and exposed to their employees in the ordinary course of business. The Fourth Amendment does not prohibit the government from obtaining this information through a subpoena rather than a warrant.

Government agents investigating tax violations issued subpoenas to two banks for Miller's account records, including financial statements and deposit slips. Miller sought to suppress these documents, arguing that they were illegally seized without a warrant in violation of the Fourth Amendment.

Justice Powell, writing for the majority, held that Miller possessed no Fourth Amendment interest in his bank records. The Court emphasized that the documents were not private papers but rather business records of the banks. The Court reasoned that the Fourth Amendment does not prohibit obtaining information a person has voluntarily conveyed to a third party, even if it was revealed for a limited purpose with the expectation that the third party would not betray the confidence. When Miller used the banks, he took the risk that the information would be conveyed to the government. The Court rejected the argument that the Bank Secrecy Act's requirements created a legitimate expectation of privacy, noting that the Act's purpose was to facilitate law enforcement access to these records. This case established the core principle of the "third-party doctrine" that information voluntarily disclosed to third parties receives no Fourth Amendment protection.

Historical Development of the Doctrine

The third-party doctrine developed through key Supreme Court cases in the 1970s, establishing the principle that information shared with others loses Fourth Amendment protection.

Foundational Cases

- ***United States v. Miller*** **(1976)**: Bank records are not protected because they are business records of the banks, not the customer's private papers
- ***Smith v. Maryland*** **(1979)**: Phone numbers dialed are not protected because the caller voluntarily conveys that information to the phone company
- ***California v. Greenwood*** **(1988)**: Trash left for collection in public is not protected because it's voluntarily given to garbage collectors

The Reasonable Expectation Standard

These cases applied the *Katz* "reasonable expectation of privacy" test, finding that people cannot reasonably expect privacy in information they share with others. The Court reasoned that by sharing information with a third party, a person assumes the risk that the third party might share that information with the government.

Statutory Protections

In response to concerns about privacy implications of the third-party doctrine, Congress enacted several statutory protections:

- **Right to Financial Privacy Act**: Requires government entities to notify customers before accessing their bank records
- **Electronic Communications Privacy Act**: Provides some protections for stored electronic communications
- **Stored Communications Act**: Restricts when electronic communication services can disclose user information

These statutes provide protections where the Fourth Amendment does not, but they generally set lower standards than the warrant requirement.

Smith v. Maryland *442 U.S. 735 (1979)*

The installation and use of a pen register to record the telephone numbers dialed from a person's phone does not constitute a "search" within the meaning of the Fourth Amendment, as a person has no legitimate expectation of privacy in information voluntarily turned over to a third party.

After a robbery, the victim received threatening calls from someone claiming to be the robber. Police identified Smith as a suspect and, without a warrant, had the telephone company install a pen register to record the numbers dialed from Smith's home phone. The register revealed that Smith called the victim, leading to his arrest and conviction.

Justice Blackmun, writing for the majority, applied the two-part test from *Katz v. United States*: (1) whether the individual exhibited an actual expectation of privacy, and (2) whether society recognizes that expectation as reasonable. The Court doubted that people generally expect privacy in the numbers they dial, noting that telephone users realize they convey phone numbers to the company for billing and other business purposes. Even if Smith did expect privacy, the Court held that this expectation was not reasonable because he voluntarily conveyed the dialed numbers to the phone company. Following *Miller*, the Court emphasized that a person has no legitimate expectation of privacy in information voluntarily turned over to third parties. This case expanded the third-party doctrine beyond financial records and established that the use of pen registers does not constitute a Fourth Amendment search.

Carpenter v. United States and Its Impact

In *Carpenter v. United States* (2018), the Supreme Court significantly limited the third-party doctrine's application to certain types of digital information, specifically cell phone location records that track a person's movements over time.

Key Holdings from Carpenter

- Obtaining seven days or more of cell-site location information (CSLI) is a Fourth Amendment search requiring a warrant
- The third-party doctrine does not extend to comprehensive, historical cell phone location records
- The deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the automatic way it is collected distinguish it from traditional third-party records

Factors That Limited the Third-Party Doctrine

The Court identified several factors that distinguish CSLI from traditional third-party records:

1. **Comprehensiveness**: CSLI provides an all-encompassing record of the phone owner's whereabouts
2. **Revealing nature**: Location information reveals the "privacies of life"
3. **Retroactivity**: Records allow government to travel back in time to track a person

4. **Pervasiveness**: Cell phones are "almost a feature of human anatomy" that most people carry at all times
5. **Involuntariness**: Location information is not truly "voluntarily" shared since cell phones log location data automatically

Narrow Ruling

Chief Justice Roberts emphasized the narrow scope of the decision:

- It does not disturb conventional application of Smith and Miller
- It does not address real-time CSLI or "tower dumps" (all information from a particular cell tower)
- It does not address other business records that might incidentally reveal location
- Traditional investigative techniques such as security cameras remain unaffected

The decision signaled a significant shift in the Court's approach to the third-party doctrine in the digital age, recognizing that some information, though technically shared with third parties, still deserves Fourth Amendment protection due to its revealing and comprehensive nature.

Carpenter v. United States *138 S. Ct. 2206 (2018)*

The government's acquisition of cell-site location information (CSLI) from wireless carriers constitutes a Fourth Amendment search, requiring a warrant supported by probable cause. The third-party doctrine does not extend to this type of comprehensive digital data that provides a detailed chronicle of a person's physical movements.

After identifying several robbery suspects, the FBI obtained court orders under the Stored Communications Act (requiring only "reasonable grounds" rather than probable cause) to collect 127 days of cell-site location records for Timothy Carpenter's phone. These records placed Carpenter's phone near four robbery locations. Carpenter moved to suppress the evidence, arguing that accessing these records without a warrant violated the Fourth Amendment.

Chief Justice Roberts, writing for the majority, held that individuals have a reasonable expectation of privacy in their physical movements as captured through CSLI, despite the fact that this information is gathered and held by third-party wireless carriers. The Court distinguished this case from Miller and Smith, emphasizing the "unique nature of cell phone location records" which provide a comprehensive chronicle of a person's movements, revealing not just locations but potentially "familial, political, professional, religious, and sexual associations." The Court noted that CSLI is not truly "shared" voluntarily since carrying a cell phone is indispensable to modern life, and the tracking occurs automatically without affirmative acts by the user. The Court also emphasized the retrospective nature of these records, allowing police to "travel back in time" to track movements. While declining to extend Smith and Miller to this new technology, the Court emphasized the narrowness of its decision, which does not disturb the application of the third-party doctrine to conventional cases or address other types of surveillance techniques.

Modern Digital Applications

After *Carpenter*, courts have grappled with applying the third-party doctrine to various forms of digital data. While *Carpenter* was intentionally narrow, its reasoning suggests potential limitations on the doctrine in other contexts.

Different Types of Digital Information

Information Type	Likely Status Post-Carpenter	Key Considerations
Email content	Likely protected	Content of communications generally requires a warrant since *United States v. Warshak*
IP address records	Likely unprotected	More like traditional phone numbers in *Smith*
Subscriber information	Likely unprotected	Basic information voluntarily provided to service providers
Web browsing history	Unclear	May reveal the "privacies of life" like CSLI, but voluntarily conveyed
Smart home data	Likely protected	Reveals detailed information about home activities
Financial app data	Unclear	More detailed than traditional bank records in *Miller*
Social media posts (public)	Unprotected	Voluntarily shared with public audience
Social media posts (private)	Unclear	Shared with limited audience, may retain some privacy protection

Unresolved Questions

The Court in *Carpenter* left many questions unresolved about the third-party doctrine's application to digital data:

- How long must location tracking last to trigger Fourth Amendment protection? *Carpenter* involved seven days, but the Court did not set a minimum threshold.
- Does the doctrine apply differently to content vs. metadata?
- How do automatic disclosures (without active user choice) affect the analysis?
- How comprehensive must information be to fall under *Carpenter* rather than *Smith/Miller*?
- How does the analysis apply to information shared with private individuals rather than businesses?

Statutory Protections in the Digital Age

Where Fourth Amendment protection remains uncertain, statutory protections become important:

- **Stored Communications Act**: Protects stored electronic communications and records
- **California Consumer Privacy Act (CCPA)**: Gives consumers right to know about data collection and opt out of data sales
- **State Constitution protections**: Some state constitutions provide greater privacy protection than the federal Constitution

The Future of the Third-Party Doctrine

The third-party doctrine continues to evolve as courts grapple with applying it to new technologies. Several trends are emerging:

1. **Narrowing Application**: Courts are increasingly reluctant to apply the doctrine broadly to all digital information

2. **Multi-Factor Analysis**: Courts consider the comprehensiveness, revealing nature, and automatic collection of information
3. **Content vs. Non-Content**: Content of communications generally receives greater protection than metadata
4. **Voluntariness Assessment**: Courts scrutinize whether sharing was truly voluntary in the digital context
5. **Privacy Expectations Evolving**: Societal expectations of privacy in digital information may be changing

Justice Sotomayor's concurrence in *United States v. Jones* (2012) suggested the Court may need to reconsider the third-party doctrine entirely, noting it is "ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."

Back to Top

Refresh Diagrams | Export to PDF