

Law of Undercover

Martin Needle
Special Counsel (Criminal Tax)
202-622-4470

Grimm v. U.S., 156 U.S. 604 (1895);
Andrews v. U.S., 162 U.S. 420 (1896)

- In these cases the Supreme Court held that the government is entitled to use decoys and conceal identities of agents in order to provide opportunities for crime.

Use of Undercover by IRS

- No difference between IRS and other law enforcement agencies using undercover
- **United States v. Little**, 753 F.2d 1420, 1436 (9th Cir. 1984) – (“Under 26 U.S.C. 7608(b) Congress granted police powers to IRS criminal investigators. These broad statutory grants of authority are clearly broad enough to encompass undercover criminal investigations which may be necessary and proper to the determination and collection of taxes, and to the general enforcement of the revenue laws.”)
- **Jones v. Berry**, 722 F.2d 443 (9th Cir. 1983)

Overview

- An investigative technique in which an IRS undercover agent or confidential informant assumes a covert identity.
- The U/C technique may be used in relation to criminal violations enforceable under the investigatory jurisdiction of the IRS (tax & money laundering)
- U/C operations may be controversial and potentially dangerous undertakings requiring significant financial and personnel resources.

Reasons for Undercover

- Develop evidence for search warrant.
- Develop affirmative acts for charging purposes.
 - 18 U.S.C. § 1956(a)(3) – Sting provision
 - 26 U.S.C. § 7206(1) – **United States v. Dahlstrom**, 713 F.2d 1423 (9th Cir. 1983).
 - 31 U.S.C. § 5331 – Failure to File Form 8300
 - 26 U.S.C. § 60501 – Structuring

Authority to Conduct Undercovers

- **26 U.S.C. § 6301** Broad powers to collect taxes
- **26 U.S.C. § 6302(b)** Broad discretion to determine reasonable devices or methods necessary and/or helpful to collect taxes
- **26 U.S.C. § 7601** Mandate to investigate those who may be liable for taxes
- **26 U.S.C. § 7608(b)** Congress granted police powers to IRS Criminal Investigation.
- **26 U.S.C. § 7608(c)** Rules relating to undercover operations, including audit and reporting requirements.

Sorrells v. United States

287 U.S. 435 (1932)

- "Artifice and stratagem" are frequently necessary to law enforcement and detection of crime.
- But decoys are not permissible to ensnare the innocent and law-abiding into the commission of crime.
- When the criminal design originates, not with the accused, but is conceived in the mind of the government officers, and the accused is by persuasion, deceitful representation, or inducement lured into the commission of a criminal act, the government is estopped by sound public policy from prosecution.
 - citing *Newman v. United States*.

Jacobson v. United States

503 U.S. 540 (1992)

- The Supreme Court held:
 - Law enforcement officers "... May not originate a criminal design, implant in an innocent person's mind the disposition to commit a criminal act, and then induce commission of the crime so that the government may prosecute."
- See, The FBI Law Enforcement Bulletin, Undercover Investigations and the Entrapment Defense, by Thomas Kukura, April 1, 1993

Jacobson v. United States

503 U.S. 540 (1992)

- The Supreme Court's rationale followed a traditional entrapment defense analysis that focuses on two basic questions:
 - (1) Did the government induce the defendant to commit the crime; and
 - (2) Assuming the government improperly induced the defendant to commit the crime, was the defendant nevertheless predisposed to commit the criminal act prior to first being approached by government agents.

Questions Relevant to Entrapment Analysis

- (1) Does the government need reasonable suspicion before targeting an individual in an undercover investigation;
- (2) What constitutes inducement;
- (3) What constitutes evidence of predisposition; and
- (4) What is the viability of the so-called outrageous government conduct defense.

Reasonable Suspicion

- There is no Federal constitutional requirement for any level of suspicion to initiate undercover operations.
- There is no constitutional right to be free of investigation and that the mere fact an undercover investigation started without reasonable suspicion does not bar the conviction of those who rise to its bait.

Inducement

- The Federal defense of entrapment requires that a defendant first establish that he was induced to commit the crime.
- If the defendant can establish inducement, the burden shifts to the government to prove the defendant was nonetheless predisposed to commit that crime.
- If the defendant cannot establish government inducement, the inquiry ends, and the Federal defense of entrapment fails.

Inducement

- Inducement generally requires more than merely establishing that an officer approached and requested a defendant to engage in criminal conduct.
- While evidence that the government engaged in persuasion, threats, coercive tactics, harassment, or pleas based on sympathy or friendship may amount to inducement, most courts require the defendant to demonstrate that the described government conduct created a substantial risk that an undisposed person or otherwise law-abiding citizen would commit the offense.

Inducement

- Inducement is not established if law enforcement officers merely provide the opportunity or facilities to commit a crime by the use of artifice and stratagem.

Predisposition

- The primary distinction between inducement and predisposition is that inducement focuses on the government's conduct, while predisposition focuses on the defendant's actions and statements.
- Once the court finds inducement, the burden shifts to the prosecution to prove beyond a reasonable doubt that the defendant was disposed to commit the criminal act prior to being approached by government agents.

Evidence of Predisposition

- (1) The character of the defendant;
- (2) Who first suggested the criminal activity;
- (3) Whether the defendant engaged in the activity;
- (4) Whether the defendant demonstrated reluctance; and
- (5) The nature of the government's inducement.

Proving Predisposition

- Prior arrest record – evidence of prior criminal activity.
- Readily agreed to participate in criminal conduct.
- Defendant admitted to engaging in the illegal activity to make a "quick buck."
- Defendant's eagerness to engage in the criminal conduct.
- Defendant's familiarity with the terminology surrounding a particular criminal venture.

Proving Predisposition

- The defendant advised the agent about the prices of various drugs in certain geographic areas, all of which indicated the defendant's knowledge and experience in the drug trade.
- However, the lack of any evidence that a defendant previously engaged in a specific crime does not conclusively preclude any predisposition to commit the crime.
- Evidence of predisposition may also be established by showing the defendant's desire to make a profit, an eagerness to participate in the criminal activity, or a quick response to the government's inducement offer.

Proving Predisposition

- Agents should carefully document any evidence of a defendant's eagerness to engage in illegal conduct.

Use of "Three and Out"

- "Three contact" authorization is a nationwide UCO that provides authority to conduct a limited number of undercover contacts to pursue leads of potential tax and other IRS approved violations.
 - **SAC Approved:** Allow UCAs to make a maximum of 3 substantive telephonic or internet contacts with a potential target.
 - **DFQ Approved:** Allow a maximum of 3 additional substantive telephonic, internet, face to face, or any combination, thereof.

Avoiding Entrapment - Rules to Remember

- (1) While reasonable suspicion is not legally necessary to initiate an undercover investigation, agents should nonetheless be prepared to articulate a legitimate law enforcement purpose for beginning such an investigation.
- (2) Agents should, to the extent possible, avoid using persistent or coercive techniques, and instead, merely create an opportunity or provide the facilities for the target to commit a crime.
- (3) Agents should document and be prepared to articulate the factors demonstrating a defendant was disposed to commit the criminal act prior to government contact.

Outrageous Government Conduct Defense

- Predicated on the Due Process clause of the 5th Amendment.
- Conduct of agents is so outrageous that due process principles would absolutely bar the government from invoking judicial processes to obtain a conviction.
- Considered to be an extraordinary defense reserved only for the most egregious circumstances.

United States v. Trigg 588 F.2d 373 (3rd Cir. 1978)

- Government informant suggested the establishment of a drug laboratory and then supplies the chemicals, equipment, and the isolated farmhouse used for manufacturing.
- The informant also did the bulk of manufacturing because the defendant did not have the requisite knowledge of the manufacturing process.

United States v. Trigg 588 F.2d 373 (3rd Cir. 1978)

- The court invoked the due process defenses and found that although proof of predisposition to commit a crime will bar application of the entrapment defense, fundamental fairness will not permit a defendant to be convicted of a crime in which law enforcement conduct was outrageous.
- The defense of outrageous government conduct is only successful in cases with a high degree of government involvement or coercion.

Undercover Review

- MOUs
- Informant Agreements
- Confidentiality Agreements
- BOP Business Contracts

Undercover Review

- Confidential Informant
 - Credibility
 - History/Background/Reason/Testify
 - Control (wired, UCA)
 - Introduce UCA
 - MOU
 - Numbered

Undercover Review

- Targets
 - History/Background/Worthiness
 - Selection Criteria

Churning Authority

- The IRS has authority to use income earned from UCOs to "offset" necessary and reasonable expenses incurred as a result of undercover activities.
- Operations that will result in earned income that can be used to offset expenses can seek the use of offset authority.

CT Counsel

- CI is required to consult the Criminal Tax attorney in all undercover operations.
- Group 1 UCO's are also reviewed by CT HQ.
- The Criminal Tax attorney's role in an undercover operation is to render legal advice on all aspects of the operation, as well as attending all pre-operational and operational meetings.
 - CCDM 38.1.1.4

Electronic Surveillance - History

- Omnibus Crime Control and Safe Streets Act of 1968 ("the Act")
 - Title III of the Act, 18 U.S.C. § 2510 *et seq.*, provided a comprehensive scheme regulating wiretapping, electronic surveillance and the interception of oral and wire communications.
- Electronic Communications Privacy Act of 1986 ("ECPA")
 - Comprehensive revision of the Act
 - Created three separate, but closely related titles.
- Communications Assistant for Law Enforcement Act of 1994
- USA Patriot Act of 2001

Electronic Surveillance

- Title I – Interception of Wire, Oral and Electronic Communications
 - 18 U.S.C. §§ 2510 – 2522
- Title II – Stored Wire and Electronic Communications
 - 18 U.S.C. §§ 2701 - 2712
- Title III – Pen Registers and Trap and Trace Devices
 - 18 U.S.C. §§ 3121 - 3127

Wire Communication

- Uses wire, cable or like method and contains human voice at some part of the transmission
 - 18 U.S.C. § 2510(1).
- The best example is a telephone call.

Oral Communication

- Any oral communication such as a conversation between two or more individuals who have a reasonable expectation of privacy.
 - 18 U.S.C. § 2510(2).

Electronic Surveillance

- Non-Consensual Monitoring of Wire/Oral Intercept (Title I).
 - Under 18 U.S.C. § 2510 (Title I), courts may authorize electronic intercept of the contents of wire and oral communications during the investigation of specific criminal offenses. (See, 18 U.S.C. § 2516 for specific offenses).
 - This statute does not authorize the interception of wire and oral communications for T-26 violations, but does authorize interception for money laundering and Bank Secrecy Act violations.
 - The Service may, however, receive Title I information from other law enforcement agents.

Electronic Surveillance – IRS Policy

- IRS Policy restricts the use of non-consensual interception of oral and wire communications to "extremely limited situations" and only in "significant money laundering investigations."
 - IRM 9.4.6.7.1(3)(a).

Non-Consensual Monitoring of Wire/Oral Interception

- IRS Agents are permitted to use wiretap evidence in their duties, such as issuing summonses, investigating tax offenses or preparing Special Agent Reports. See, 18 U.S.C. § 2517.
- Agents are permitted to use the evidence in a grand jury, court or any other proceeding, or they may disclose it via testimony.
- Prior to such use, the agent must obtain a derivative use order that must be based upon the court's finding that the evidence of non-specified crime (i.e., tax offense) was properly intercepted.

Electronic Communications

- Electronic communications are those which do not contain the human voice at any point during the transmission and are defined as any transfer of signs, signals, written images, sound, data or intelligence of any nature.
- This includes systems such as digital pagers, electronic mail, electronic bulletin boards, computer-to-computer transmissions, and faxes.

Electronic Communications

- 18 U.S.C. § 2516(3) allows for the interception of electronic communications when such interception may provide or has provided evidence of any federal felony, including T26 offenses.
- To intercept such communications, electronic communication intercept orders must be based upon an application and an affidavit, which are reviewed by the Criminal Tax attorney.

Title I - Application

- Made in writing (supported by affidavit) upon oath or affirmation to a judge.
 - 18 U.S.C. § 2518(1).
- Authorization:
 - Attorney General, Deputy Attorney General, Associate Attorney General, Assistant Attorney General, or Specially Designated Attorney General.
 - 18 U.S.C. § 2516(1).

Title I - Requirements

- Duration
 - 30 days
 - 18 U.S.C. § 2518(5)
- Minimization
 - Terminate once objective obtained
 - Privileges
 - Must constantly monitor to determine relevancy

Non-Consensual Monitoring of Wire/Oral Interception

- The Criminal Tax attorney reviews the legality of the Title I order and advises the SAC in a memorandum. The U.S. Attorney's Office obtains the appropriate derivative use order.

Stored Electronic Communications (Title II)

- Stored electronic communications and transactional records include storage of electronic messages both before and after transmission. Also included are Remote Computer Services, where electronic data is processed and/or stored by third-parties.
- The IRS may gain access to such communications via authorization obtained pursuant to 18 U.S.C. § 2703.

Stored Electronic Communications (Title II)



- If the data has been stored for less than 180 days, a search warrant is required.
- If the data has been stored over 180 days or is stored in a Remote Computer Service:
 - If notice to the subscriber is not given, a search warrant must be obtained;
 - If notice is given to the subscriber, a disclosure court order or grand jury/administrative trial subpoena is required.

Stored Electronic Communications (Title II)



- The subscriber is usually notified of government access, unless upon a showing of good cause, the court delays notice for up to 90 days.
- The Criminal Tax attorney should review the legal sufficiency of the affidavit in support of an application for search warrant or court order.

Stored Electronic Communications



- Many electronic communication services only store data for short periods of time.
- Special agents can issue a preservation (or 2703(f)) letter that is signed by the SA or AUSA.
- The letter requires providers to retain records for 90 days, with another 90 day extension period.

Title III – Pen Registers and Trap and Trace



- A pen register is a mechanical instrument attached to a phone line that records outgoing numbers dialed on a particular line and registers incoming calls.
- A trap and trace device records the telephone numbers from incoming calls to a particular telephone line.

Title III – Pen Registers and Trap and Trace



- Exempt from Title I requirements because it does not seize the contents of communications.
- Subject to 4th Amendment requirements when you need physical intrusion for installation.
- General requirement to obtain a court order
 - Standard for obtaining a pen register or trap and trace is relevancy, not P/C. 18 U.S.C. § 3122
 - Upon approval of SAC, the AUSA provides magistrate with sworn application and a draft order.

Consensual Monitoring



- Consensual monitoring occurs when at least one party to a conversation agrees to have the conversation monitored.
- Because a party to the conversation consents to the recording, this activity does not implicate Title I.
- No court order is required.

Consensual Monitoring – Authorization



- SAC generally has authority to approve telephonic consensual monitoring requests.
- DFO required when the request relates to an U/C.
- Chief/Deputy Chief approval required where recording device is to be installed in a place or manner that will create risk of inadvertent prohibited non-consensual monitoring.
- DOJ approval required for judges, politicians, prisoner, and diplomats.