Parallel Construction: A Defense Attorney's Guide to Discovering and Challenging Original Source Evidence in Criminal Investigations

Jessica Carmichael
CARMICHAEL ELLIS & BROCK | Alexandria, Virginia

I. What is parallel construction?

a. Government learns of information through warrantless surveillance
b. Provides that information to law enforcement
c. Law enforcement recreates the investigation as though the source of the investigation originated in another way.

II. Natasha Babazadeh, *Concealing Evidence: "Parallel Construction," Federal Investigations, and the Constitution*, 22 Va. J.L. & Tech. 1 (2018)

a. Parallel construction is the process of building a separate--and parallel--evidentiary basis for a criminal investigation. The process is undertaken to conceal the original source of evidence, which may have been obtained unlawfully. Clandestinely used for decades, this process raises serious constitutional questions.
b. Parallel construction allows law enforcement agencies to capitalize on sensitive or secret national security techniques in the domestic criminal context, without any form of oversight or accountability.
c. The result: parallel construction insulates surveillance techniques from judicial review, undermines checks and balances, and deprives individuals of the privacy benefits that court review would require. It also undermines fundamental principles of due process. Parallel construction enables law enforcement agencies to engage in questionable investigative practices, the concealment of which deprives criminal defendants of any challenges they might raise and prevents courts from reviewing the constitutionality of the practice in the first place.

III. John Shiffman & Kristina Cooke, *Exclusive: U.S. directs agents to cover up program used to investigate Americans*, REUTERS (Aug. 5, 2013)

a. "A secretive U.S. Drug Enforcement Administration unit is funneling information from intelligence intercepts, wiretaps, informants and a massive database of telephone records to authorities across the nation to help them launch criminal investigations of Americans."
b. Anonymous senior DEA official: "Parallel construction is a law enforcement technique we use every day."

IV. What are some of the surveillances used?

a. NSA/Intelligence agencies
b. Foreign partnerships

c. Stingrays/surveillance devices
d. Companies

V. Intelligence Collection – NSA, 702 FISA

a. PRISM
    i. Leaked by Edward Snowden in 2013
    ii. Bulk collection of NSA records from private electronic data belonging to users of major internet services like Gmail, Facebook, Outlook, and others from 2007-2015 under Section 702. Bulk collection allegedly ended by legislation 2015
    iii. Section 702 was set to expire Dec. 31, 2023. In March 2024, Senators Dick Durbin and Kevin Cramer, filed an amendment to the FISA Reauthorization Bill that would require the government to obtain a warrant from the Foreign Intelligence Surveillance Court (FISC) before reviewing the contents of Americans' private communications that get swept up in Section 702 surveillance. *See* U.S. Senate, Committee on the Judiciary, Durbin, *Lee Introduce Bipartisan SAFE Act to Reform FISA Section 702* (March 14, 2024). Senator Durbin explained that "[i]f the government wants to spy on my private communications or the private communications of any American, they should be required to get approval from a judge, just as our Founding Fathers intended in writing the Constitution." Ellen Nakashima et al, *Congress extends controversial warrantless surveillance law for two years*, Washington Post (April 20, 2024).
b. *Section 702: What It Is & How It Works*, Center for Democracy and Technology, https://cdt.org/wp-content/uploads/2017/02/Section-702.pdf
    i. Unlike "traditional" FISA surveillance, Section 702 does not require that the surveillance target be a suspected terrorist, spy, or other agent of a foreign power. Section 702 only requires that the targets be non-U.S. persons located abroad, and that a "significant purpose" of the surveillance be to obtain "foreign intelligence information" (the primary purpose of the surveillance can be something else entirely).
    ii. PRISM collection: the government collects all communications content to or from a targeted selector (such as an email address) directly from U.S.-based electronic communications service providers (such as Apple or Google). The NSA receives all raw (unminimized) PRISM-collected information and may also send such raw data to the CIA and FBI.
    iii. Upstream collection: the government collects all internet transactions that contain communications to, from, or "about" a targeted selector as the transactions flow through network gateways controlled by U.S.-based providers. Only the NSA may receive raw Upstream-collected information, but it may send such information to the CIA and FBI once it has gone through the NSA's minimization process.

c. Amber Phillips, *What's the database the FBI misused to seek info on Jan. 6 suspects, BLM arrestees?* The Washington Post, (May 19, 2023)
    i. The FBI is in hot water for misusing a powerful surveillance tool nearly 300,000 times in 2020 and early 2021, including to search for information about Americans linked to the Jan. 6, 2021, attack on the U.S. Capitol or arrested during Black Lives Matter protests.
    ii. The FBI is supposed to search the 702 database for information about U.S. residents or companies only when the FBI agent or analyst has a reason to believe such a query may generate foreign intelligence information or evidence of a crime. The FBI is supposed to follow strict procedures because using the database allows the bureau to skip the usual step of getting a warrant from a federal court to collect information on Americans.
    iii. In 2020 and early 2021, the FBI misused the database more than 278,000 times by conducting searches that didn't follow Justice Department rules, often to look for information on Americans who don't have connections to national security, The Washington Post's Devlin Barrett reports. The FBI has searched the database for "crime victims, Jan. 6 riot suspects, people arrested at protests after the police killing of George Floyd in 2020 and — in one case — 19,000 donors to a congressional candidate, according to a newly unsealed court document," he reports. (full court document here: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/21/2021_FISC_Certification_Opinion.pdf)
d. Names of some other NSA surveillance programs: Stellar Wind, Prism,EvilOlive, ShellTrumpet

VI. Intelligence Collection- EO 12333

a. John Napier Tye, *Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans,* The Washington Post (July 18, 2014).
    i. John Napier Tye served as section chief for Internet freedom in the State Department's Bureau of Democracy, Human Rights and Labor from January 2011 to April 2014. He is now a legal director of Avaaz, a global advocacy organization.
    ii. I believe that Americans should be even more concerned about the collection and storage of their communications under Executive Order 12333 than under Section 215.
    iii. Bulk data collection that occurs inside the United States contains built-in protections for U.S. persons, defined as U.S. citizens, permanent residents and companies. Such collection must be authorized by statute and is subject to oversight from Congress and the Foreign Intelligence Surveillance Court. The statutes set a high bar for collecting the content of communications by U.S. persons. For example, Section 215

permits the bulk collection only of U.S. telephone metadata — lists of incoming and outgoing phone numbers — but not audio of the calls.

iv. Executive Order 12333 contains no such protections for U.S. persons if the collection occurs outside U.S. borders. Issued by President Ronald Reagan in 1981 to authorize foreign intelligence investigations, 12333 is not a statute and has never been subject to meaningful oversight from Congress or any court. Sen. Dianne Feinstein (D-Calif.), chairman of the Senate Select Committee on Intelligence, has said that the committee has not been able to "sufficiently" oversee activities conducted under 12333.

v. Before I left the State Department, I filed a complaint with the department's inspector general, arguing that the current system of collection and storage of communications by U.S. persons under Executive Order 12333 violates the Fourth Amendment, which prohibits unreasonable searches and seizures. I have also brought my complaint to the House and Senate intelligence committees and to the inspector general of the NSA.

vi. Keith Alexander, a former NSA director, has said publicly that for years the NSA maintained a U.S. person e-mail metadata program similar to the Section 215 telephone metadata program. And he has maintained that the e-mail program was terminated in 2011 because "we thought we could better protect civil liberties and privacy by doing away with it." Note, however, that Alexander never said that the NSA stopped collecting such data — merely that the agency was no longer using the Patriot Act to do so. I suggest that Americans dig deeper.

b. Elizabeth Goitein, *How the CIA Is Acting Outside the Law to Spy on Americans* (Feb. 15, 2022).

i. most foreign intelligence surveillance actually takes place under EO 12333, not FISA. That means it is subject to no statutory constraints whatsoever, and there is no judicial review or oversight. EO 12333 does place some limits on surveillance, but not shockingly, its rules are much more permissive than those Congress established in FISA. Bulk collection is just one example — it's banned under FISA but permitted under EO 12333.

ii. What stops the CIA from poring through the data looking for Americans' information? Let's be honest: nothing. The CIA's internal rules from 2017 say the information sought must be "related to a duly authorized activity of the CIA," as determined by. . . the CIA. The FBI has similar rules limiting its searches of data obtained under FISA Section 702. Year after year, the Foreign Intelligence Surveillance Court finds that FBI agents have violated these rules—and that's when there's a court actually watching them.

iii. The CIA's rules also say that CIA officers should document their purpose in running searches for Americans' information. But according to staff members of the Privacy and Civil Liberties Oversight Board, these rules, despite having been finalized five years ago and released with great fanfare, have not yet been "implemented."

iv. And suppose for a moment that the CIA did restrict itself to searches designed to retrieve foreign intelligence (a limitation that would certainly satisfy the CIA's rules, despite the fact that EO 12333 defines "foreign intelligence" to include literally any information about the actions of any foreign person). Since when does the Fourth Amendment allow government agencies to help themselves to Americans' private data as long as they're conducting agency business? Should police be able to search your house without a warrant as long as they're investigating a crime?

VII. Intelligence Collection- Section 215 of Patriot Act

a. Bulk collection of more than 534 million phone records under Section 215 in 2017 and more than 434 million in 2018.
   i. https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf
b. Expired in 2020, but still contains exceptions permitting the intelligence community to use the law for investigations that were ongoing at the time of expiration or to investigate "offenses or potential offenses" that occurred before the sunset.
   i. https://www.eff.org/deeplinks/2020/12/section-215-expired-year-review-2020

VIII. Intelligence Collection - DEA's Hemisphere

a. Scott Shane and Colin Moynihan, *Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s*, The New York Times (Sept. 1, 2013).
   i. For at least six years, law enforcement officials working on a counternarcotics program have had routine access, using subpoenas, to an enormous AT&T database that contains the records of decades of Americans' phone calls.
   ii. Hemisphere covers every call that passes through an AT&T switch — not just those made by AT&T customers — and includes calls dating back 26 years, according to Hemisphere training slides bearing the logo of the White House Office of National Drug Control Policy. Some four billion call records are added to the database every day, the slides say; technical specialists say a single call may generate more than one record. Unlike the N.S.A. data, the Hemisphere data includes information on the locations of callers.
   iii. The slides were given to The New York Times by Drew Hendricks, a peace activist in Port Hadlock, Wash. He said he

had received the PowerPoint presentation, which is unclassified but marked "Law enforcement sensitive," in response to a series of public information requests to West Coast police agencies.

iv. "All requestors are instructed to never refer to Hemisphere in any official document," one slide says. A search of the Nexis database found no reference to the program in news reports or Congressional hearings.

v. [Government] said, the phone data is stored by AT&T, and not by the government as in the N.S.A. program. It is queried for phone numbers of interest mainly using what are called "administrative subpoenas," those issued not by a grand jury or a judge but by a federal agency, in this case the D.E.A.

vi. Brian Fallon, a Justice Department spokesman, said in a statement that "subpoenaing drug dealers' phone records is a bread-and-butter tactic in the course of criminal investigations." Mr. Fallon said that "the records are maintained at all times by the phone company, not the government," and that Hemisphere "simply streamlines the process of serving the subpoena to the phone company so law enforcement can quickly keep up with drug dealers when they switch phone numbers to try to avoid detection." He said that the program was paid for by the D.E.A. and the White House drug policy office but that the cost was not immediately available.

b. Dave Maass, *Before and After: What We Learned About the Hemisphere Program After Suing the DEA*, Electronic Frontier Foundation (Dec. 19, 2018).

i. Hemisphere has faded somewhat from the headlines since it was first revealed. That was long enough for officials to rebrand the program "Data Analytical Services," making it even less likely to draw scrutiny or stick in the memory.

ii. AT&T embeds employees with police agencies in at least three hubs: Los Angeles, Houston, and Atlanta. These employees run the software that searches and analyzes AT&T massive phone database. Cops (usually working drug cases) from around the country contact their regional hub to get the records, and federal officials can query Hemisphere without first getting permission from a judge. The system was reportedly especially useful for tracking people when they switched phones.

IX. Companies

a. Ex. Dep't of Justice: FOR IMMEDIATE RELEASE, Monday, June 2, 2014, *U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator*

i. Invaluable technical assistance was provided by Dell SecureWorks and CrowdStrike. Numerous other companies also provided assistance, including facilitating efforts by victims to remediate the damage to their computers inflicted by Gameover

Zeus. These companies include Microsoft Corporation, Abuse.ch, Afilias, F-Secure, Level 3 Communications, McAfee, Neustar, Shadowserver, Anubis Networks, Symantec, Heimdal Security, Sophos and Trend Micro. (Available at https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware)

b. Trend Micro: Our work with U.S. agencies
    i. As a leading voice and global citizen in the fight against cybercrime, we are proud to support law enforcement globally. Trend Micro shares strategic and tactical threat intelligence with U.S. Government Law Enforcement, including the FBI, U.S. Secret Service, and Homeland Security Investigations. We participate in threat and vulnerability research, joint reports with the U.S. Secret Service, and frequent collaborations with FBI's InfraGard and the U.S. Secret Service Electronic Crimes Task Force. Read The Evolution of Cybercrime and Cyber Defense, our joint research paper with the U.S. Secret Service (Available at https://www.trendmicro.com/en_us/business/capabilities/solutions-for/federal-government/agencies-stories.html)

X. Stingrays

a. Adam Bates, Stingray: *A New Frontier in Police Surveillance, Cato Institute*, at 5, Jan. 25, 2017
    i. Stingray surveillance devices are cellular site simulators — they are portable, military-grade surveillance devices that mimic the signal of a cell phone tower in order to force cell phones in the area to connect. Once a phone connects, the officer can download information from the phone or track its location.
    ii. Cell site simulators may be known by a variety of different brand names, including: "Triggerfish," Stingray," "Hailstorm," and "KingFish." They may also be referred to generically as "IMSI catchers," referring to a cell phone's "International Mobile Subscriber Identity"
    iii. Stingrays can be used to locate "cell phones to within six feet," including in a user's home or apartment

b. NDAs
    i. law enforcement agencies have a history of secrecy regarding the use of cell site simulators. Not only are law enforcement loath to confirm their use, they are also often contractually obligated to withhold information under their Nondisclosure Agreements – even in response to a court order. (Available at https://www.cehrp.org/tags/stingray/).
    ii. Emails from litigation in Florida on this matter show law enforcement directives to redraft investigation reports to conceal the use of a cell site simulator by simply calling it a "confidential

source." (Available at https://www.aclu.org/sites/default/files/assets/aclu_florida_stingray_police_emails.pdf)

c. LEO need a warrant to use a stingray
    i. "[W]hen the government uses cell-site simulators (often called 'stingrays') to *directly* intercept CSLI instead of obtaining CSLI records from phone companies, the Department of Justice requires a warrant." *United States v. Graham*, 824 F.3d 421, 426 n.4 (4th Cir. 2016)(emphasis in original)
    ii. "The Department recognizes that the collection of precise location information in real time implicates different privacy interests than less precise information generated by a provider for its business purposes." *United States v. Lambis*, 197 F. Supp 3d 606, 611 (S.D.N.Y 2016) (citing Deputy Assistant Attorney General Richard Downing Testifies Before House Oversight and Government Reform Committee at Hearing on Geolocation Technology and Privacy, 2016 WL 806338 (Mar. 2, 2016)).

XI. Ways to identify possible parallel construction

a. Not obvious how case started
b. Reports use passive tense
    i. "investigation revealed"
c. Report skips step
d. " defendant was located"
e. Vague language
    i. LEO ID'ed defendant through "legal processes"
f. Anonymous tips
g. Pretexual traffic stops
h. Consents
i. Defense investigation
j. Gut instincts
    i. "when law enforcement finds—for example—20 kilograms of drugs in a vehicle during a stop, 'The chances of it being a random traffic stop … [are] unlikely in my opinion.'" –HRW Report

XII. How to leverage

a. Prosecutors likely will not know.
b. "Although these cases rarely involve national security issues, documents reviewed by Reuters show that law enforcement agents have been directed to conceal how such investigations truly begin - not only from defense lawyers but also sometimes from prosecutors and judges." *Exclusive: U.S. directs agents to cover up program used to investigate Americans*, REUTERS
c. Motions to compel (Court, how will you assess the Fourth Amendment issues?)
d. *Roviaro* motion

e. Motions to suppress
    i. What was the probable cause for the search?
    ii. What was the "reason to believe" the defendant would be there?
    iii. Working arrangement/joint venture
f. Any other motions that shift burden to prosecution
g. Cross examination at trial

XIII. What could this do?

a. Lead to suppression of evidence
b. Shake the prosecutor's faith in the LEO on the case
c. Cause Court to question the prosecution
d. Dismissal
    i. Former ODNI general counsel Robert Litt told Human Rights Watch, and Arthur Rizer implied, that prosecutors may drop cases in order to avoid revealing sources or methods. "At the end of the day, if the Intelligence Community says, 'You can't risk this information, you need to dismiss the case,' that carries the day," Litt said. –HRW Report

XIV. Examples in caselaw

a. Human Rights Watch identified, the disclosure of a "wall stop" was inadvertent (evidence emerged in a New Mexico federal trial that an officer had mentioned a "whisper stop from DEA" to a dispatcher while unaware that he was being recorded).
b. *United States v. Sheridan*, case no. 1:10-cr-00333 (D. NM), Defendant's Motion to Suppress and Memorandum in Support Thereof (doc. 26), filed March 18, 2010, pp.2-3
c. A defendant who had been convicted in Arizona state court only found out the traffic stop in his case was a "whisper stop" requested by the DEA after his conviction, when pertinent records were later disclosed in a California federal court.
d. *Arizona v. Wakil*, case no. CR 2011-00530 (Arizona Superior Court, Coconino County), Petition for Post-Conviction Relief, August 21, 2014; *Arizona v. Wakil*, Minute Entry: Oral Argument on Petition for Post Conviction Relief, November 6, 2014.
e. "That afternoon, Agent Kenneybrew contacted GSP and asked them to prepare a 'whisper stop,' in which ICE tells a local law enforcement agency that a vehicle contains drugs or other contraband but asks the local agency to develop its own probable cause for the stop to avoid compromising the federal investigation. Around 8:00 p.m., the red Volkswagen returned to the truck stop, and Sanders returned to the tractor-trailer and followed the red Volkswagen out of the parking lot. Agent Kenneybrew notified GSP, which subsequently stopped the tractor-trailer for traffic and equipment violations." *United States v. Sanders*, 668 F.3d 1298, 1303 (11th Cir. 2012)

XV. Conclusion

a. "[A] defendant whose attorney is aware of parallel construction and asks hard questions may avoid imprisonment—while a defendant whose attorney is less savvy may not. " – HRW Report
b. Look for it
c. Use it
d. And if I can help, contact me, jessica@carmichaellegal.com

XVI. Resources

a. Secondary Sources

i. Sarah St.Vincent, *Dark Side: Secret Origins of Evidence in US Criminal Cases*, Human Rights Watch (Jan. 9, 2018) https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases
ii. Natasha Babazadeh, *Concealing Evidence: "Parallel Construction," Federal Investigations, and the Constitution*, 22 Va. J.L. & Tech. 1 (2018)
iii. FOIA Response Documents: https://s3.documentcloud.org/documents/1011382/responsive-documents.pdf
iv. John Shiffman & Kristina Cooke, *Exclusive: U.S. directs agents to cover up program used to investigate Americans*, REUTERS (Aug. 5, 2013)
v. Adam Bates, Stingray: A New Frontier in Police Surveillance, CATO Institute (Jan. 25, 2017) https://www.cato.org/policy-analysis/stingray-new-frontier-police-surveillance#cite-43
vi. Yomna N, Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks, EFF (June 28, 2019) https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks

b. Sample Motions

i. *O'Shaughnessy*, D. Or. 3:16cr51, ECF No. 545
ii. *Mohammad*, N.D. OH, 3:15cr358, ECF No. 131
iii. *Thomas*, E.D. Pas, 2:15cr171, ECF No. 72
iv. *Alimehmetl*, S.D.NY, 1:16cr398, ECF No. 61

c. Court Orders

i. *Lambis*, S.D.NY, 1:15cr734, ECF No. 30
ii. *Hasbajmmi*, E.D.NY, 1:11cr623, ECF No. 85