HUMAN RIGHTS WATCH

Dark Side

Secret Origins of Evidence in US Criminal Cases

Printed in the United States of America
ISBN: 978-1-6231-35645
Cover design by Rafael Jimenez

Human Rights Watch defends the rights of people worldwide. We scrupulously investigate abuses, expose the facts widely, and pressure those with power to respect rights and secure justice. Human Rights Watch is an independent, international organization that works as part of a vibrant movement to uphold human dignity and advance the cause of human rights for all.

Human Rights Watch is an international organization with staff in more than 40 countries, and offices in Amsterdam, Beirut, Berlin, Brussels, Chicago, Geneva, Goma, Johannesburg, London, Los Angeles, Moscow, Nairobi, New York, Paris, San Francisco, Sydney, Tokyo, Toronto, Tunis, Washington DC, and Zurich.

For more information, please visit our website: http://www.hrw.org

JANUARY 2018

ISBN: 978-1-6231-35645

Dark Side

Secret Origins of Evidence in US Criminal Cases

Summary

> Judge: [I]f, you know, there was an illegal search … followed by a legal search, but that was only obtained because now that you had the illegal search, you knew something about [the case], that would be a concern to the Court.… And that is the fruit of the poisonous tree, potentially.
>
> Prosecutor: I respectfully dispute that point.… [I]n fact, I don't have any concern about that.
>
> —Hearing transcript, United States v. Lara (Northern District of California), December 2013

> We have in our country a Fourth Amendment and Fourth Amendment rights.… That's a bedrock principle of our system. Essentially, this practice is an attempt to circumvent that.
>
> —Jessica Carmichael, Virginia-based defense attorney who has represented a client in a case of suspected parallel construction, discussing the practice with Human Rights Watch in July 2017

In the United States today, a growing body of evidence suggests that the federal government is deliberately concealing methods used by intelligence or law enforcement agencies to identify or investigate suspects—including methods that may be illegal. It does so by creating a different story about how agents discovered the information, and as a result, people may be imprisoned without ever knowing enough to challenge the potentially rights-violating origins of the cases against them.

Through a practice known as "parallel construction," an official who wishes to keep an investigative activity hidden from courts and defendants—and ultimately from the public—can simply go through the motions of re-discovering evidence in some other way. For example, if the government learned of a suspected immigration-related offense by a person in Dallas, Texas, through a surveillance program it wished to keep secret, it could ask a Dallas police officer to follow the person's car until she committed a traffic violation, then pull her over and start questioning her—and later pretend this traffic stop was how the investigation in her case started.

Due to parallel construction, defendants in criminal cases across the country may be experiencing serious infringements of their rights without their knowledge. The United States Constitution draws on lessons learned from the abuses of the British colonial era in placing firm restrictions on how the government can behave when it wants to prove someone has done something wrong. It establishes criteria for rights-respecting searches and seizures, requires the prosecution to turn over to the defense any evidence favorable to the accused, and demands that all trials and proceedings take place in accordance with "due process"—that is, fundamental fairness. However, parallel construction—when sustained through the end of proceedings—means defendants cannot learn about, and therefore cannot challenge, government actions that violate these or other rights.

In creating fictions to keep potentially questionable investigative activities out of sight, the government also avoids an important deterrent to official misconduct. When law enforcement or intelligence agencies break the law, judges typically prohibit prosecutors from introducing evidence that was obtained as a result of those illegal operations. This is one of the main incentives agents have to respect rights. Parallel construction removes this incentive by deliberately rendering those agents' actions invisible to courts and defendants, and the resulting lack of accountability risks turning constitutional rights into little more than words on paper.

This impact is not limited to criminal defendants. If government agents can potentially create privacy-violating, discriminatory, or otherwise unlawful programs or patterns of behavior in secret and without facing any negative consequences, the rights of every member of the public are in jeopardy. Taken to its worst logical conclusion, parallel construction risks creating a country in which people and communities are perpetually vulnerable to investigations based on prejudice, vast illegal operations, or official misconduct, but have no means of learning about these problems and holding agents to account.

Of particular concern is the potential use of parallel construction to hide intelligence surveillance programs. Modern US intelligence surveillance is as sweeping as it is secretive, and a lack of disclosure of the use of such surveillance in criminal investigations means wide-ranging or acute civil liberties violations may go unnoticed.

Parallel construction also means judges may never evaluate whether government uses of constantly evolving surveillance techniques adhere to the US Constitution and laws

adopted by Congress, as is their role in the US system. For example, if the government were to identify a suspect in a robbery by scrutinizing a store's security video using a new but flawed facial recognition technology it does not want to reveal, it could send an informant to talk to the suspect and report what he said—then suggest in court records that this conversation was how the investigation began. Such possible uses of parallel construction are especially troubling in human rights terms because new technologies may be inaccurate (including, in the case of facial recognition software, for people of certain racial or ethnic groups) or raise new legal concerns. Unless judges are aware that such new technology has been used, they will not be able to assess whether the technology violates rights.

Virginia-based defense attorney Jessica Carmichael, who has represented a client in a case that gave rise to concerns about potential parallel construction, told Human Rights Watch the practice "flies in the face of everything that our justice system stands for." Referring to the Fourth Amendment to the US Constitution, which is intended to protect the population against abusive searches and seizures by the authorities, she continued, "Essentially, this practice is an attempt to circumvent that. It's a way that defendants can't challenge the evidence and the way that it was obtained." Other defense attorneys told Human Rights Watch that parallel construction "encourages law enforcement to be duplicitous" and risks destroying the essence of Fourth Amendment protections.

Human Rights Watch investigated parallel construction from April 2016 to October 2017 using interviews, court records, documents disclosed by the government, and media reports. In this report we detail how the practice:

- Is a technique that, the evidence suggests, is employed frequently and possibly even daily;
- Has roots in strained and untested government interpretations of US Supreme Court and other cases—cases that in fact have never explicitly provided license for officials to deliberately avoid telling defendants the truth about investigative methods in order to conceal practices that might raise legal concerns;
- May be employed by a range of federal agencies responsible for investigating suspected violations of criminal and immigration law;
- In particular, is employed by a part of the Drug Enforcement Administration ("DEA") known as the Special Operations Division ("SOD"), at least part of which has been nicknamed "the Dark Side" and which the evidence suggests is responsible for

passing tips to various law enforcement bodies with the expectation that those tips will not be revealed in court;

- Regularly relies on pretextual stops and searches of vehicles—an exercise of police powers that is sometimes known as a "wall stop" or "whisper stop" and that risks becoming unlawfully coercive;
- May also rely on other tactics, such as attempts to find incriminating evidence by obtaining a suspect's consent to a search of his or her person or belongings, requests for call records (which do not require a warrant under US law), closed proceedings under the Classified Information Procedures Act, or the use of less-controversial intelligence surveillance methods to conceal more controversial forms;
- Is at least sometimes used in investigations involving relatively minor offenses;
- Prevents courts from providing oversight over surveillance and other investigative methods, and therefore from deterring law enforcement misconduct; and
- Is facilitated by prosecution tactics for resisting defense attorneys' efforts to find out how the cases against their clients truly originated, including prosecution claims that agencies such as the NSA are not part of the prosecution "team" and that prosecutors therefore are not required to find out if such agencies were involved in the investigation.

The government appears to have developed legal justifications for parallel construction based on theories with which at least some US courts might agree in individual cases. These theories appear to hinge on exceptions to the "exclusionary rule"—a court-developed doctrine under which judges generally will not allow prosecutors to introduce evidence obtained thanks to illegal behaviors. (Such evidence is known as "fruit of the poisonous tree.") They may also hinge on prior cases in which courts have allowed the government to conceal the identities of human informants.

However, in making any secret determinations about whether it can legally withhold information about its activities, the government essentially claims for itself the judge's role. Moreover, except in instances in which the government ultimately decides on its own initiative to reveal that it has engaged in parallel construction, court documents reviewed by Human Rights Watch suggest that defendants and their lawyers face a low likelihood of being able to find out whether parallel construction has occurred (and challenge the

lawfulness of the government's actions in this area). Where the possible use of intelligence surveillance is concerned, the discovery of such information as part of criminal proceedings is essentially the only way a defendant can find out whether she or he may have been unlawfully monitored, since US doctrines related to "standing" (that is, the ability to establish a right to sue by showing that one has been or will be harmed by a government action) make it difficult for individuals who lack strong evidence that they were surveilled to bring suit.

The report concludes that parallel construction violates the right to fair trial proceedings. It also facilitates other potential human rights violations by hiding them from defendants, judges, and the public. Depending on the circumstances, these violations may include infringements on privacy rights (as in the case of any unlawful surveillance), defendants' right of access to any evidence the government holds that is favorable to them, and the entitlement to a remedy for government abuses. By shielding official decisions and actions from view, parallel construction may also conceal law enforcement or intelligence activities that violate rights in a discriminatory manner.

"Society wins not only when the guilty are convicted, but when criminal trials are fair," the US Supreme Court wrote more than 50 years ago in *Brady v. Maryland*. Parallel construction means society loses: people facing the loss of their liberty may receive unfair trials, and government activities that may violate the human rights of significant numbers of people—or even, as in the case of large-scale surveillance programs, much of the population—are shielded from view.

This report recommends that the US executive branch prohibit all government departments and agencies from engaging in or contributing to parallel construction efforts, and disclose all policies related to the concealment of sources or evidence. The Office of the Director of National Intelligence ("ODNI") should also publicly and fully disclose all policies and legal interpretations of the intelligence agencies that may affect criminal defendants or others involved in proceedings before US courts or tribunals. Additionally, the US Congress should require the disclosure to criminal defendants of complete information about the origins of the investigations in their cases, with special procedures as necessary to address classified information or information whose disclosure may jeopardize the safety of identifiable human informants.

Human Rights Watch further urges federal and state courts, whenever the circumstances suggest that parallel construction may have occurred, to direct the prosecution to inquire into and disclose any previously unrevealed investigative sources or techniques that were employed as part of the investigation. Defense attorneys, too, should be alert to the possibility that their clients' cases may have stemmed from undisclosed activities.

As a concealment method, parallel construction poses unique research challenges; the point of the practice is to ensure that no one outside of government knows it has taken place. Human Rights Watch's investigation nevertheless indicates that this use of secret evidence may be occurring regularly in cases throughout the country—cases in which the person accused of an offense remains innocent until proven guilty and faces a potentially life-altering prison term. The report concludes that action is needed immediately to end an aspect of the US justice system that is, in the words of multiple defense attorneys who spoke with Human Rights Watch, a lie.

Methodology

From April 2016 to October 2017, Human Rights Watch investigated the issue of parallel construction through a combination of interviews, analyses of court opinions and records, and assessments of government documents.

For the purposes of this research, Human Rights Watch has defined "parallel construction" to include deliberate efforts by US government bodies, as part of a criminal investigation or prosecution, to conceal the true origins of evidence by creating an alternative explanation for how the authorities discovered it.

For example, if the government learned of a piece of information by intercepting and reading an e-mail, then sent a confidential human informant to the e-mail sender's door to try to get him or her to repeat the same information so the government would not have to reveal the interception of the message, this would constitute parallel construction in accordance with our understanding. Another hypothetical example—drawn from allegations made by the defense in a federal case in New Mexico[1]—would be a government agent's secret search of a piece of luggage, followed by a deliberate effort to persuade the luggage's owner to consent to a search of the bag just as if the first search (the one the government does not wish to admit having done) had never happened.

This report includes a focus on the potential use of parallel construction to conceal warrantless surveillance activities due to particular human rights concerns about those activities. However, as discussed herein, officials may also use parallel construction to conceal sources of information that are not necessarily related to warrantless surveillance, such as a tip from a human informant or a wiretap that takes place pursuant to a court order.

As part of this investigation, Human Rights Watch assessed judicial decisions, transcripts, briefs, and/or other court records from 95 relevant US federal and state criminal cases. Some of these cases were identified through outreach to defense attorneys, while others

[1] *United States v. Grobstein*, case no. 1:13-cr-00663 (D. NM), Defendant's Motion to Suppress (doc. 44), May 6, 2013, https://www.hrw.org/sites/default/files/supporting_resources/201711us_motion_to_suppress.pdf.

were located through database searches or media coverage, or shared with Human Rights Watch by the American Civil Liberties Union.

To better understand the practice of parallel construction and its consequences, Human Rights Watch also conducted 24 interviews with defense attorneys, current and former US officials, and experts from civil society groups.

To uncover evidence concerning the government's legal and policy justifications for parallel construction as well as the history and nature of the practice, we examined several hundred pages of documents that executive branch agencies have released following Freedom of Information Act ("FOIA") requests or by their own initiative. Some of the most significant of these included policies and other materials declassified and released by ODNI; historical documents posted in the online FOIA reading room of the Central Intelligence Agency ("CIA"); and trainings and other documents obtained under FOIA by the American Civil Liberties Union, the Electronic Frontier Foundation, and the journalist CJ Ciaramella.[2] We submitted our own FOIA requests concerning intelligence surveillance and parallel construction to 22 federal agencies in January 2017 and were still awaiting final responses from many at the time this report was finalized.[3]

Additionally, we have incorporated information obtained by journalists from media outlets such as Reuters, which published a groundbreaking article on parallel construction in August 2013.[4] In some sections of the report, we have utilized (primarily as corroborating evidence) a blog post by a former New York state prosecutor that had strong indicia of authenticity, although efforts to arrange an interview with the author prior to the finalization of this report were unsuccessful.

---

[2] See "DEA policies on 'parallel construction,'" post to Muckrock (blog), undated, https://cdn.muckrock.com/foia_files/1-23-14_MR6434_RES_ID13-00541-F_1.pdf (accessed October 31, 2017) (hereinafter "Muckrock documents").

[3] See "Human Rights Watch Asks US about Use of Secret Surveillance for Drug, Immigration Purposes," Human Rights Watch, January 23, 2017, https://www.hrw.org/news/2017/01/23/human-rights-watch-asks-us-about-use-secret-surveillance-drug-immigration-purposes.

[4] John Shiffman and Kristina Cooke, "Exclusive: US directs agents to cover up program used to investigate Americans," *Reuters*, August 5, 2013, http://www.reuters.com/article/us-dea-sod/exclusive-u-s-directs-agents-to-cover-up-program-used-to-investigate-americans-idUSBRE97409R20130805 (accessed October 31, 2017) (hereinafter "Shiffman and Cooke").

Several discussions in this report draw on materials concerning US intelligence surveillance that were disclosed by former NSA contractor Edward Snowden beginning in 2013, or on US diplomatic cables that Army soldier Chelsea Manning (then known as Bradley) disclosed to the media organization WikiLeaks in 2010.

The CIA, Federal Bureau of Investigation ("FBI"), NSA, and ODNI responded to requests for comment by referring Human Rights Watch to the Justice Department.[5] The Justice Department declined our request for an interview, stating in an e-mail that "as a general matter, [the Department] does not comment on issues surrounding investigative sources and methods, or related litigation."[6] The DEA also declined to provide comments.[7] However, this report extensively quotes and describes materials produced by US government lawyers.

The issues addressed in this report include only those pertaining to information the government does or does not disclose to defendants, who may challenge the legality of the government's techniques for gathering the information, and the role of judges, who are responsible for making determinations in this area. The report does not address prosecutors' decisions about which evidence to present to juries at trial.

[5] Email from Ben Huebner, Privacy and Civil Liberties Officer, Central Intelligence Agency, to Human Rights Watch, August 9, 2017; Email from Andrew C. Ames, National Press Office, Federal Bureau of Investigation, to Human Rights Watch, August 17, 2017; Email from Vanee M. Vines, Public and Media Affairs Office, National Security Agency/Central Security Service, to Human Rights Watch, August 25, 2017; Email correspondence between Human Rights Watch and Alexander W. Joel, Chief, Office of Civil Liberties, Privacy, and Transparency, Office of the Director of National Intelligence, August 16, 2017.

[6] Email from Wyn Hornbuckle, Deputy Director, Office of Public Affairs, Department of Justice, to Human Rights Watch, September 22, 2017.

[7] Email from Katherine M. Pfaff, National Media Affairs, Office of Congressional and Public Affairs, Drug Enforcement Administration, to Human Rights Watch, August 8, 2017.

I. Background

In August 2013, the wire service Reuters published an article revealing the deliberate use of parallel construction to conceal the original sources of evidence.[8] Focusing on the DEA, journalists John Shiffman and Kristina Cooke found that a "secretive" unit known as the Special Operations Division was "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." Documents they had obtained, the reporters wrote, showed that "federal agents are trained to 'recreate' the investigative trail to effectively cover up where the information originated."[9]

In Reuters' account, an anonymous senior DEA official depicted parallel construction as "a bedrock concept" that is "decades old" and that the government employs daily.[10] A former federal prosecutor who spoke with Human Rights Watch on the condition of anonymity said of the use of pretextual stops and searches of vehicles for parallel construction purposes, "Does it bother me a little? Yeah. But if it's gonna stop 100 keys [kilograms of drugs] from getting on the street, it's okay by me. I didn't make the rules. I just play by them."[11]

US civil liberties groups, however, have decried parallel construction, with the American Civil Liberties Union characterizing it as a "dangerous constitutional runaround" and the Electronic Frontier Foundation calling it "intelligence laundering."[12]

The government's justifications and methods for carrying out parallel construction, and some rights-based objections to the practice, are grounded in certain key features of US law:

---

[8] Shiffman and Cooke.

[9] Ibid.

[10] Ibid.

[11] Human Rights Watch interview with a former US federal prosecutor who requested anonymity, United States, 2016.

[12] Matthew Harwood and Jay Stanley, "Power Loves the Dark," post to American Civil Liberties Union (blog), May 19, 2016, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/power-loves-dark (accessed October 31, 2017); Hanni Fakhoury, "DEA and NSA Team Up to Share Intelligence, Leading to Secret Use of Surveillance in Ordinary Investigations," post to Electronic Frontier Foundation (blog), August 6, 2013, https://www.eff.org/deeplinks/2013/08/dea-and-nsa-team-intelligence-laundering (accessed October 31, 2017).

- The Fourth Amendment to the US Constitution establishes protections against unreasonable searches and seizures by the authorities, as well as a requirement that warrants be based upon probable cause to believe that wrongdoing has occurred or will soon occur.[13]
- The Constitution also establishes in the Fifth and Fourteenth Amendments that the government cannot deprive individuals of their "liberty … without due process of law."[14]
- Judges in US courts will normally prohibit prosecutors from introducing evidence the government obtained thanks to illegal activities.[15] Such evidence is known as "fruit of the poisonous tree," and the rule is known as the "exclusionary rule."[16] The US Supreme Court has characterized the purpose of the exclusionary rule as the deterrence of future law enforcement misconduct.[17]
- There are exceptions to the "fruit of the poisonous tree" doctrine, and some of these appear to form part of the government's legal underpinning for parallel construction. Under these exceptions, evidence the authorities originally located through an illegal action may still be admissible.
- One exception to the "fruit of the poisonous tree" doctrine, known as the "independent source" exception, arises where "a later, lawful seizure is *genuinely independent* of an earlier, tainted [i.e., unlawful] one."[18] Other exceptions to the "fruit of the poisonous tree" doctrine arise if the government "inevitably" would have discovered the evidence in some other manner "without reference to" the unlawful action, or if its discovery of the evidence through lawful methods was sufficiently "attenuated" from the unlawful behavior.[19]
- One of the best-documented parallel construction methods is pretextual stops and searches of vehicles in the hopes that officers will find incriminating items such as drugs. A key legal basis for these stops is *Whren v. United States*, in which the US Supreme Court held that a law enforcement officer may stop a car whenever the officer has probable cause to believe a traffic violation has occurred, and that it

[13] United States Constitution, Fourth Amendment.

[14] United States Constitution, Fifth, and Fourteenth Amendments.

[15] *Weeks v. United States*, 232 U.S. 383 (1914); *Mapp v. Ohio*, 367 U.S. 643 (1961).

[16] *Nardone v. United States*, 308 U.S. 338 (1939); *Wong Sun v. United States*, 371 U.S. 471 (1963); *Mapp v. Ohio*.

[17] See, e.g., *Mapp v. Ohio*, p. 656; *Illinois v. Krull*, 480 U.S. 340, 347 (1987).

[18] *Murray v. United States*, 487 U.S. 533, 542 (1988) (emphasis added).

[19] *Nix v. Williams*, 467 U.S. 431, 448 (1984); *Nardone v. United States*; *Wong Sun v. United States*.

does not matter whether the officer has some other, unrelated motive for carrying out the stop.[20] However, *Whren* concerned only the legality of the traffic stop itself and did not address any application of the "fruit of the poisonous tree" doctrine to investigative activities that led to the stop.

- During a traffic stop, an officer may use various means of searching the vehicle for contraband or other evidence that gives rise to probable cause to believe that a criminal offense has been or is being committed (thus justifying an arrest). For example, the officer may ask for consent to search the car.[21] (As scholars have pointed out, individuals regularly provide what is legally regarded as valid consent, even when it is not in their interest to do so.)[22] Even in the absence of consent, the officer may use a drug-detecting dog to carry out a "canine sniff" of the vehicle.[23] Consent may also serve as a legal basis for other warrantless searches; for example, an officer may approach a bus passenger and ask for consent to search his or her luggage, even though in most circumstances the officer would not otherwise be permitted to carry out the search without a warrant.[24]
- A crucial protection for defendants was established by the US Supreme Court in *Brady v. Maryland*, in which the court found that the Constitution's due process provisions require the prosecution to disclose any exculpatory evidence to the defense (that is, any evidence that is "favorable" to him or her).[25] The court has also found that the prosecution "has a duty to learn of any favorable evidence known to the others acting on the government's behalf in the case, including the police."[26]

The government may be using parallel construction to conceal surveillance activities, although it may also use the practice to prevent other types of sources from being disclosed. Where surveillance is concerned, important concepts and historical background include:

---

[20] *Whren v. United States*, 517 U.S. 806 (1996).

[21] See, e.g., *Ohio v. Robinette*, 519 U.S. 33 (1996).

[22] See, e.g., Alafair S. Burke, Consent Searches and Fourth Amendment Reasonableness, *Florida Law Review* vol. 67 (2016), pp. 521-531, available at http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1247&context=flr (accessed November 6, 2017).

[23] *Illinois v. Caballes*, 543 U.S. 405 (2005)

[24] On warrantless luggage searches, see *Bond v. United States*, 529 U.S. 334 (2000).

[25] *Brady v. Maryland*, 373 U.S. 83 (1963).

[26] *Kyles v. Whitley*, 514 U.S. 419 (1995).

- The US government collectively describes its intelligence agencies as the "Intelligence Community."[27] In addition to the NSA and CIA, these include—among others—the FBI, the DEA's Office of National Security Intelligence, and the Department of Homeland Security's Office of Intelligence and Analysis.[28] The emergence of these various intelligence bodies has created decades-long controversies about the role they should play in monitoring people and events in the United States and their proper relationship to domestic law enforcement.[29] Some of these controversies are rooted in a history of various forms of unnecessary and/or discriminatory monitoring of African-Americans, Native Americans, women's rights advocates, political dissidents, and others.[30] State and local law enforcement bodies, too, have faced repeated outcries over allegedly unlawful monitoring of minorities.[31]
- Normally, US law enforcement agents may only intercept or demand the content of telephone or internet communications if they first obtain a warrant or order from a court. This requirement stems from the Fourth Amendment and is found in a 1968 law commonly known as the Wiretap Act, which has since been amended to cover electronic communications.[32]
- However, the US Supreme Court ruled in 1979 that the Fourth Amendment does not require officers to obtain a warrant before seeking records of telephone calls (other than the content of the conversation).[33] The logic of this ruling continues to underpin various forms of warrantless collection of metadata (that is, non-content

---

[27] See "Members of the IC," Office of the Director of National Intelligence, https://www.dni.gov/index.php/what-we-do/members-of-the-ic (accessed November 6, 2017).

[28] Ibid.

[29] See, e.g., David S. Kris and J. Douglas Wilson, *National Security Investigations & Prosecutions 2d* (Thomson West, 2012), vol. 1, pp. 42-44, 63-87; vol. 2, pp. 5-13.

[30] Ibid., vol. I, pp. 38-44; *United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Intelligence Activities and the Rights of Americans* (1976), Report no. 94-755, Book II, pp. 6-12 (hereinafter "Church Committee Report"), available at http://www.aarclibrary.org/publib/contents/church/contents_church_reports_book2.htm (accessed October 17, 2017).

[31] See, e.g., Matt Apuzzo and Adam Goldman, "After Spying on Muslims, New York Police Agree to Greater Oversight," *New York Times*, March 6, 2017, https://www.nytimes.com/2017/03/06/nyregion/nypd-spying-muslims-surveillance-lawsuit.html (accessed November 6, 2017); Denis C. Theriault, "'Shameful and dangerous': Civil rights group rips Black Lives Matter surveillance," *OregonLive/Oregonian*, April 12, 2016, http://www.oregonlive.com/politics/index.ssf/2016/04/shameful_and_dangerous_civil_r.html (accessed November 6, 2017).

[32] "Title III of The Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act)," Department of Justice, Sept. 13, 2013, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1284 (accessed November 6, 2017); 18 U.S.C. § 2511.

[33] *Smith v. Maryland*, 442 U.S. 375 (1979).

information about internet or telephone communications) in the US. Since the government does not need a warrant to obtain call records, demands for such records may be used as a form of parallel construction to hide some other activity.[34]

- The government's creation of large, warrantless databases of telephone records, as well as its warrantless collection of cell-phone location data, are also some of the activities parallel construction may have been used to conceal.[35]
- The US Supreme Court has also ruled that, at least in some circumstances, the Fourth Amendment does not apply to "activities of the United States directed against aliens in foreign territory or in international waters."[36] Thanks in part to this holding, the executive branch has concluded that it is entitled to carry out extremely large warrantless intelligence surveillance programs, as long as those programs do not specifically target a "US person" (a category that includes US citizens; lawful permanent residents, also known as green-card holders, and some corporations and associations).[37] When conducting such surveillance, the government believes it has the power to gather Americans' communications "incidentally" and to search them without a warrant.[38] Whistleblowers and independent experts have indicated that the scale of the "incidental" surveillance of US persons' communications could be large.[39]
- In some circumstances, US federal law explicitly requires that defendants or other individuals involved in proceedings be notified of surveillance employed in their cases.[40] However, officials have indicated that they do not believe they are required to notify defendants of any investigative use of surveillance data obtained under one of the country's most important intelligence surveillance authorities

---

34 See Part II below.

35 Ibid.; Tim Cushing, "Stingray Memo From FBI To Oklahoma Law Enforcement Tells PD To Engage In Parallel Construction," *TechDirt*, May 9, 2016, https://www.techdirt.com/articles/20160507/10052134369/stingray-memo-fbi-to-oklahoma-law-enforcement-tells-pd-to-engage-parallel-construction.shtml (accessed November 7, 2017).

36 *United States v. Verdugo-Urquidez*, 494 U.S. 259, 266 (1990).

37 50 U.S.C. § 1801(i).

38 See, e.g., *United States v. Mohamud*, case no. 14-30217 (9th Cir.), Answering Brief of Plaintiff-Appellee (doc. 53-2), pp. 102 et seq.

39 Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (Washington, DC, 2014), available at https://www.pclob.gov/library/702-Report.pdf, p. 9 (accessed November 6, 2017) (hereinafter "PCLOB Report"); Brief of *Amicus Curiae*, United States Foreign Intelligence Surveillance Court, Oct. 16, 2015, p. 11, available at https://www.aclu.org/foia-document/brief-fisc-amicus-curiae-amy-jeffress?redirect=foia-document/brief-amicus-curiae (accessed November 6, 2017).

40 E.g., 18 U.S.C. § 2518(8)(d).

(Executive Order 12333), and controversies continue as to whether the government is complying fully with its obligation to notify defendants of surveillance under a controversial provision of the Foreign Intelligence Surveillance Act ("FISA"), Section 702.[41] Executive Order 12333, Section 702 of FISA, and other US intelligence surveillance authorities are explained in greater detail in the Annex to this report.

While the legal justifications for parallel construction largely appear to lie in some of the court-acknowledged exceptions to the "fruit of the poisonous tree" doctrine, the historical origins of the practice are more difficult to discern. However, declassified documents suggest that debates within the executive branch about the possibility of deliberately using alternative investigative methods to prevent the disclosure of the original sources of information extend back to at least the mid-1970s. At the time, following revelations about discriminatory or otherwise abusive domestic monitoring (see above), the intelligence agencies perceived "a sense of prohibition against cooperation" between themselves and law enforcement bodies.[42] "This is especially true," a committee of intelligence officials wrote in a 1976 report, "in the narcotics area."[43] The agencies also worried that if defendants made motions in court for the disclosure of information about the evidence against them in court cases, "sensitive SIGINT" (signals intelligence, meaning surveillance) methods could be publicly revealed.[44]

To begin addressing the latter issue, the 1976 report recommended a review of "the feasibility of … enabling negative responses to information requests or motions for discovery of 'electronic surveillance' data on the grounds that such SIGINT is properly classified and essential national security information not used for evidentiary or prosecutive [*sic*] purposes."[45] In other words, the report suggests that at least some officials were attempting to determine how they could refuse defense motions asking the

---

[41] Charlie Savage, "Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide," *New York Times*, August 13, 2014, https://mobile.nytimes.com/2014/08/14/us/politics/reagan-era-order-on-surveillance-violates-rights-says-departing-aide.html (accessed November 6, 2017); Patrick C. Toomey, "Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance—Again?," post to Just Security (blog), Dec. 11, 2015, https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again (accessed October 31, 2017).

[42] "Impact of Executive Order 11905 and Implementing Guidelines on Signals Intelligence Agencies of the United States," 1976, CIA Freedom of Information Act Electronic Reading Room document no. CIA-RDP79M00467A001100190008-2, p. 3.

[43] Ibid.

[44] Ibid.

[45] Ibid., p. 4.

government to turn over surveillance data. A revised version of the report circulated the following year suggested:

> The need to protect sensitive intelligence sources and methods which provide foreign narcotics information from public disclosure can conflict with the legal requirement that the sources of evidence used in the prosecution of a narcotics trafficker in a U.S. court be disclosed to the defense. In order to preserve future access to sensitive sources and methods which contribute significant information to the overall narcotics [intelligence] collection effort, agencies involved should work together more closely to ensure that such information is not used in the prosecution of a trafficker. If it appears that a U.S. prosecution or potential prosecution might invite disclosure of a sensitive source, the agency or agencies involved should notify the Department of Justice as quickly as possible so that all prosecutorial alternatives can be fully explored.[46]

A 1983 document proposed that a panel should:

> [r]ecommend intelligence support processes for drug enforcement that will enable drug agencies to develop evidence independently and reduce the likelihood that intelligence sources and methods will be regarded [as] essential to a criminal defendant's case; in effect, build a firebreak in the evidentiary [trail] leading to sources and methods.[47]

This approach matches the tactic now commonly known as "parallel construction."

---

[46] Critical Collection Problems Committee, "CCPC Study on Intelligence Activities against Illicit Narcotics Trafficking," September 1976, CIA Freedom of Information Act Electronic Reading Room document no. CIA-RDP86M00638R000100050001-0, p. 5.

[47] "Terms of Reference: CIPC Narcotics Working Group's Panel on the Use of Classified Intelligence Information by Drug Enforcement Agencies," Sept. 19, 1983, CIA Freedom of Information Act Electronic Reading Room doc. no. CIA-RDP90B00612R000100060019-7, available at https://www.hrw.org/sites/default/files/supporting_resources/cipc_narcotics_working_group.pdf. The word "trail" in the quotation above from this document reads "trial" in the original text; this appears to be a copyist's error, but either reading provides the same sense of the suggested practice.

II. Parallel Construction in Action

Interviews and documentary research conducted by Human Rights Watch regarding the current practice of parallel construction indicate that the technique may be common. Evidence further suggests that a range of federal agencies may be employing it to conceal a variety of intelligence and law enforcement sources, in some instances including warrantless surveillance.

A. Federal Agencies that Request or Carry Out Parallel Construction

1. Agencies Other Than the DEA

While the DEA and its SOD have been the focus of much of the public attention regarding parallel construction, and while parallel construction in the context of drug investigations may be frequent, Human Rights Watch's research suggests that other federal agencies also employ the technique.

In particular, a search of a major legal database using terms associated with pretextual traffic stops (a parallel construction technique, although not the only one) revealed references in published US federal and state court opinions to requests for such stops by—or to conceal the investigations of—entities other than the DEA.[48] These include the FBI,[49] Immigration and Customs Enforcement ("ICE")[50] and its Homeland Security Investigations unit,[51] and the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF").[52] Meanwhile, Reuters has reported that an Internal Revenue Service ("IRS") manual available to the agency's personnel between 2005 and 2007 contained an entry describing parallel

[48] Search terms Human Rights Watch used for this purpose included "wall stop," permutations of "wall-off stop" and "walled-off stop," and "whisper stop." The opinions we located in this manner occasionally included references to other salient opinions that did not employ these terms.

[49] *United States v. Benard*, 2010 U.S. Dist. LEXIS 100189 (D. Utah 2010); *United States v. Munoz*, 2015 U.S. Dist. LEXIS 159443 (D. Utah 2015).

[50] *United States v. Sanders*, 668 F.3d 1298 (11th Cir. 2012); *United States v. Son*, case no. 1:12-cr-00042 (N.D. GA), Suppression Hearing (Transcript) (doc. 35), filed June 2, 2012, p. 9 (testimony by state trooper Matt Moorman that "ICE wanted me to perform a traffic stop on the vehicle. It is what we call a whisper stop").

[51] *United States v. Bruce*, 2013 U.S. Dist. LEXIS 170948 (D. Ariz. 2013); *United States v. Browne*, 219 F. Supp. 3d 1030 (D. Mont. 2016).

[52] *United States v. Mitchell*, 2008 U.S. Dist. LEXIS 95512 (D. Mass. 2008).

construction and instructing personnel to use various methods to "recreate"—and thereby avoid disclosing—information provided by the DEA's SOD.[53]

The FBI has also used non-disclosure agreements to direct local police departments to employ "additional and independent investigative means and methods" to avoid revealing the collection of telephone-related metadata using cell-site simulators (commonly known as "Stingrays" after the brand name of one type of equipment used for this purpose).[54] Cell-site simulators behave like mock cellular phone towers, deceiving mobile telephones in the vicinity into connecting and sharing information with them as if they were real towers.[55] The technology is reportedly "capable of intercepting data from hundreds of people's cellphones at a time," and the constitutionality of using it without a warrant remained open to debate at the time of publication.[56]

Additionally, case records and government documents suggest that the executive branch may have engaged in parallel construction in at least some cases involving NSA surveillance. For example, a 2009 report by several government offices of inspectors general (made publicly available in 2015) found that, beginning in 2003, a special FBI team

---

53 John Shiffman and David Ingram, "Exclusive: IRS manual details DEA's use of hidden intel evidence," Reuters, August 7, 2013, http://www.reuters.com/article/us-dea-irs/exclusive-irs-manual-detailed-deas-use-of-hidden-intel-evidence-idUSBRE9761AZ20130807 (hereinafter "Shiffman and Ingram").

54 Jenna McLaughlin, "FBI Told Cops to Recreate Evidence from Secret Cell-Phone Trackers," *Intercept*, May 5, 2016, https://theintercept.com/2016/05/05/fbi-told-cops-to-recreate-evidence-from-secret-cell-phone-trackers/ (accessed December 9, 2017); Jessica Glenza and Nicky Woolf, "Stingray spying: FBI's secret deal with police hides phone dragnet from courts," *Guardian*, April 10, 2015, https://www.theguardian.com/us-news/2015/apr/10/stingray-spying-fbi-phone-dragnet-police (accessed December 9, 2017).

55 "Cell-site Simulators: Frequently Asked Questions," Electronic Frontier Foundation, undated, https://www.eff.org/sls/tech/cell-site-simulators/faq (accessed November 6, 2017).

56 Brad Heath, "Police secretly track cell phones to solve routine crimes," *USA Today*, August 23, 2015, https://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/ (accessed November 6, 2017). The Justice Department issued a policy in 2015 requiring federal law enforcement to obtain warrants before using cell-site simulators, subject to exceptions; however, the policy does not apply to state or local authorities, although some states have adopted laws restricting the use of these devices. Department of Justice, "Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology," undated, https://www.justice.gov/opa/file/767321/download (accessed November 6, 2017); Department of Justice, "Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators," September 3, 2015, https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators (accessed November 6, 2017); Electronic Frontier Foundation, "Cell-site Simulators: Frequently Asked Questions." At the time this report was finalized, the US Supreme Court was considering a case, *Carpenter v. United States*, that does not directly address but may have profound implications for understandings of whether the warrantless use of Stingrays is constitutional. See "ACLU at Supreme Court Wednesday to Argue in Cellphone Tracking Case," American Civil Liberties Union, November 27, 2017, https://www.aclu.org/news/aclu-supreme-court-wednesday-argue-cellphone-tracking-case (accessed December 19, 2017).

was assigned to share information from a classified NSA surveillance program codenamed Stellar Wind with their colleagues at the Bureau "without disclosing that the NSA was the source of the information or how the NSA acquired the information."[57] When sharing the information, the team instructed recipients that it could not be "incorporated into any … court proceeding."[58]

The Justice Department has also failed to notify defendants at the outset of their cases that surveillance data obtained by the NSA and/or the FBI under a controversial warrantless intelligence surveillance law, Section 702 of FISA (a successor to the Stellar Wind program), had been involved in the investigations leading to their prosecutions. In at least one such case, the government has contended that prior to a Justice Department policy change, it simply "had not considered the particular question" of whether surveillance under a somewhat less controversial provision of FISA—one entailing an individualized court order—"could also be considered to be derived from prior collection" under Section 702.[59] The defense replied that "[t]he government's claim that it was unaware" that constitutional doctrines concerning evidence that may be tainted by illegality applied to information derived from Section 702 "strains credulity."[60]

In another case, defendant Agron Hasbajrami had already pleaded guilty when the government notified him that Section 702 surveillance had been employed in his case. Judge John Gleeson permitted Hasbajrami to withdraw his guilty plea, describing the government's previous provision of notice of surveillance under a FISA order—but not Section 702—as "misleading."[61]

---

[57] Offices of the Inspectors General of the Department of Defense et al., *Report on the President's Surveillance Program*, vol. 1, July 10, 2009, p. 272, available here: https://www.nytimes.com/interactive/2015/04/25/us/25stellarwind-ig-report.html?_r=0.

[58] Ibid., p. 273.

[59] *United States v. Mohamud*, case no. 3:10-CR-00475 (D. Or.), Government's Response to Defendant's Motion for Full Discovery Regarding Surveillance (doc. 491), February 13, 2014, p. 7.

[60] *United States v. Mohamud* (D. Or.), Reply to Government's Response to Motion for Full Discovery Regarding the Facts and Circumstances Underlying Surveillance (doc. 496), February 27, 2014.

[61] *Hasbajrami v. United States*, case no. 1:11-cr-00623 (E.D. NY), Order (doc. 85), filed October 3, 2014, p. 6.

As this report was being finalized, the *Intercept* reported that it had identified a case in which the government notified a defendant of monitoring under a FISA order without ever disclosing that the investigation had also relied on Section 702 surveillance data.[62]

2. The DEA and its Special Operations Division

As noted above, Reuters has identified a DEA unit known as the Special Operations Division as disseminating intelligence and other information in a manner that is not revealed during prosecutions. Human Rights Watch's research suggests that the SOD may include a "Dark Side" responsible for carrying out some of the division's potentially controversial operations.

In general, the DEA's rationale for its practice of parallel construction appears to be much the same as that expressed in government documents from the 1970s and 1980s (see above). DEA training documents obtained by the journalist CJ Ciaramella under the Freedom of Information Act in 2013 and reviewed by Human Rights Watch explain "parallel reconstruction" by pointing to the idea that while "[u]nclassified material can be used in court," classified materials—including sources, methods, and technologies—"must be protected."[63] One training notes:

> Our friends in the military and intelligence community never have to prove anything to the general public. They can act upon classified information without ever divulging their sources or methods to anyway [*sic*] outside their community. If they find Bin Laden's satellite phone and then pin point his location, they don't have to go to a court to get permission to put a missile up his nose.
>
> We are bound, however, by different rules.
>
> Our investigations must be transparent. We must be able to take our information to court and prove to a jury that our bad guy did the bad things

[62] Trevor Aaronson, "NSA Secretly Helped Convict Defendants in U.S. Courts, Classified Documents Reveal," *Intercept*, November 30, 2017, https://theintercept.com/2017/11/30/nsa-surveillance-fisa-section-702/ (accessed December 8, 2017).
[63] Muckrock documents, p. 9 of the complete PDF.

> we say he did. No hiding here. However, we are also bound to protect certain pieces of information so as to protect the sources and methods.
>
> To use it…., we must properly protect it.[64]

In other words, the training indicated that if the DEA wished to continue to benefit from information the government was gathering through certain methods, it needed to prevent the public disclosure of those methods.

A 2007 DEA presentation Ciaramella obtained sought to introduce participants to "legally acceptable methodologies for handling this problem"—that is, the problem of how to use intelligence information in law enforcement investigations "without disclosing or unduly risking disclosure of sensitive or classified [Intelligence Community] information."[65] "Our government has worked out procedures to accommodate the sharing of IC [Intelligence Community] information with [law enforcement agents] for criminal investigations," the training notes state[66]—and one of these procedures is parallel construction, which "can shield information that might otherwise be discoverable in circumstances where the IC and [law enforcement agents] have focused on the same individual or groups of individuals."[67]

a. The nature of the SOD

The DEA contains a Special Operations Division established in 1994; according to congressional testimony by Derek S. Maltz, who then served as the SOD's special-agent-in-charge, the purpose of the SOD's creation was to facilitate the sharing of intelligence among law enforcement and intelligence bodies.[68] In an interview with Human Rights Watch, Maltz described the SOD as "an operational law enforcement center" intended to "coordinate different transnational crime threats to the country and utilize different agency representatives to put together the pieces of the puzzle."[69]

---

[64] Ibid.; see also p. 11 of the complete PDF.

[65] Ibid., p. 14 of the complete PDF.

[66] Ibid. at p. 16 of the complete PDF.

[67] Ibid. at p. 39 of the complete PDF.

[68] Derek S. Maltz, "Narcoterrorism and the Long Reach of U.S. Law Enforcement, Part II," Statement before the House Subcommittee on Terrorism, Nonproliferation, and Trade, November 17, 2011, p. 4, https://www.dea.gov/pr/speeches-testimony/2012-2009/111117_testimony.pdf (accessed November 6, 2017).

[69] Human Rights Watch telephone interview with Derek S. Maltz, August 3, 2017.

"What we used to see back in the old days," Maltz explained, "was [that] when these cartels based in Colombia were sending drugs in to the US," they used operatives located in a wide variety of geographical locations. The DEA therefore needed a centralized team to coordinate its field operations and cases.[70]

The idea behind the SOD, he said, "is to piece together the different elements of a criminal network" that is allegedly responsible for crime in the United States "and use all tools of national power to attack the network."[71]

Similarly, Arthur Rizer, a former federal prosecutor who worked at the SOD from 2010 to 2013, described the SOD to Human Rights Watch as "like a clearinghouse for information for very large prosecutions."[72]

Maltz told Human Rights Watch that the division incorporates representatives from perhaps 30 different agencies, including partners from the United Kingdom, Canada, and Australia. (Along with the United States, these three countries and New Zealand are members of an international intelligence-sharing arrangement known as the Five Eyes.[73]) Two former DEA Special Agents who had worked in the SOD offered descriptions consistent with Maltz's during a DEA panel discussion in 2015, depicting the entity as "basically a task force"—one that incorporates agencies ranging from the FBI and US Customs and Border Protection to the New York City Police Department and foreign partners from the same countries Maltz later named.[74] Similarly, Reuters reported that the SOD includes "[t]wo dozen partner agencies" such as the "CIA, NSA, Internal Revenue Service and Department of Homeland Security."[75]

---

[70] Ibid.

[71] Ibid.

[72] Human Rights Watch interview with Arthur Rizer, Washington, DC, June 8, 2017.

[73] Privacy International, "The Five Eyes," undated, https://www.privacyinternational.org/node/51 (accessed November 6, 2017).

[74] "DEA Museum Lecture Series: The History of the Special Operations Division" (Transcript), April 22, 2015, pp. 5, 20-21, https://www.deamuseum.org/wp-content/uploads/2015/08/042215-DEAMuseum-LectureSeries-MLS-SOD-transcript.pdf (accessed November 7, 2017) (hereinafter "DEA Museum Lecture").

[75] Shiffman and Cooke.

The first special-agent-in-charge of the SOD, Michael Horn, later described the Division as having adopted a groundbreaking approach at the time of its creation: "I think it was the first time that … a federal law enforcement agency really effectively used the work of the Intelligence side. It was … intelligence-led policing."[76] Nathaniel Burney, a former state narcotics prosecutor in Manhattan, has claimed in a public blog post to have interacted with the SOD in the late 1990s and early 2000s and has explained:

> A lot of international drug trafficking takes place outside our borders, so the idea was to take advantage of intelligence data to make the drug war more effective. You just can't use the intelligence data in court. So SOD was formed as a way to make the information known, without compromising criminal investigations…. [W]hat the SOD does is get evidence from sources that can never see the light of day in court—usually from intelligence services here and abroad…. If something comes up about some big drug trafficking — not at all uncommon to hear about in the intelligence world— then the SOD hears about it. Then they clue in law enforcement. It's up to law enforcement to figure out how to gather the evidence legally.[77]

Historically, one of the SOD's key functions has been to "exploit[] communications-related data for law enforcement purposes."[78] A 2007 report by the Justice Department's Office of the Inspector General explained that according to the DEA:

> [T]he most effective means of ascertaining the breadth of a drug trafficking operation is to track the communication between the parties involved. The SOD is a repository for phone numbers used or called by persons who are part of a DEA investigation. The SOD uses a database to collect these phone numbers and can connect cases with hits on the same phone

[76] Privacy International, "The Five Eyes."

[77] Nathaniel Burney, "On the DEA's Special Operations Division," post to *The Criminal Lawyer* (blog), August 5, 2013, http://burneylawfirm.com/blog/2013/08/05/on-the-deas-special-operations-division-2/ (accessed Oct. 31, 2017) (hereinafter "Burney blog").

[78] U.S. Department of Justice, Office of the Inspector General, "Review of the Organized Crime Drug Enforcement Task Forces Fusion Center," March 2014, p. 2, https://oig.justice.gov/reports/2014/e1402.pdf (accessed November 6, 2017).

numbers. This allows the DEA to link cases investigated by different offices across the country and throughout the world.[79]

In April 2015, *USA Today* revealed that for many years, the Justice Department and the DEA had "amassed logs of virtually all telephone calls from the USA to as many as 116 countries linked to drug trafficking," including Mexico and Canada. According to the newspaper's account, the DEA's SOD had passed tips based on this program to agents in the field while avoiding disclosing the existence of the program itself—potentially a way of encouraging parallel construction. (The Justice Department reportedly ended this program in September 2013.)[80]

US diplomatic cables from 2009 and 2010 that were later disclosed to WikiLeaks show DEA agents asking the SOD to provide information concerning telephone numbers furnished by foreign government entities in relation to drug investigations.[81]

Today, the data the SOD gathers, stores, and searches could extend well beyond telephone call records. A 2004 NSA document that Snowden revealed describes the NSA and DEA as having "a vibrant two-way information sharing relationship" and mentions "the critical supporting role that NSA continues to play in key DEA operations to disrupt the flow of narcotics to our country and thwart other, related crimes."[82] While this document is no longer recent, former Justice Department attorney Melanie Reid wrote in a 2015 article that "[a]s it currently stands, there is nothing prohibiting the DEA from utilizing NSA intercepts

---

[79] U.S. Department of Justice, Office of the Inspector General, "The Drug Enforcement Administration's International Operations (Redacted)," February 2007, https://oig.justice.gov/reports/DEA/a0719/chapter4.htm#51 (accessed November 6, 2017) (citation omitted).

[80] Brad Heath, "U.S. secretly tracked billions of calls for decades," *USA Today*, April 7, 2015, https://www.usatoday.com/story/news/2015/04/07/dea-bulk-telephone-surveillance-operation/70808616/ (accessed November 6, 2017).

[81] "Action Request for Subscriber, Tolls and Indices Checks for DEA SOD, DEA Country Offices; Kabul, India, Egypt, Dubai and Canberra," June 23, 2009, https://wikileaks.org/plusd/cables/09ISLAMABAD1375_a.html (accessed November 6, 2017); "UI-09-0003/WEH1F/Sarov, Nosir/Telephone Toll Information Related to the Sarov Drug Trafficking Organization," April 24, 2009, https://wikileaks.org/plusd/cables/09DUSHANBE488_a.html (accessed November 6, 2017); "UI-09-0003/YEH1K/Saraf, Haji Nasir, Tajik Ministry of Interior Toll and Subscriber Information Related to the Haji Nasir Saraf DTO," June 2, 2009, https://wikileaks.org/plusd/cables/09DUSHANBE669_a.html (accessed November 6, 2017).

[82] "DEA – The 'Other' Warfighter," Apr. 20, 2004, https://search.edwardsnowden.com/docs/DEA%E2%80%93the%E2%80%9COther%E2%80%9DWarfighter2014-05-19nsadocs (accessed November 6, 2017).

under FISA or 702 or E.O. 12,333 as tips to initiate criminal investigations."[83] As explained in the Annex to this report, these intelligence authorities empower the government to gather content as well as records (metadata) of communications. Additionally, Burney's blog post refers to "[w]iretaps conducted without regard to Title III"—that is, the Wiretap Act, which requires law enforcement to get a warrant for the monitoring of telephone or Internet conversations—"because they're not intended for criminal prosecution," although Human Rights Watch has been unable to confirm the occurrence or nature of such "wiretaps."[84]

It appears that the SOD's early days were not without controversy: according to Horn, the FBI—one of the SOD's earliest partners—"initially didn't think … some of our techniques and tools were being … legally implemented."[85] However, he added, "When they started seeing some success, they … kind of changed their mind. And … they came on board."[86]

It may have been these doubts about the legality of the SOD's operations that earned the division (or some element of it) the moniker "the Dark Side." Human Rights Watch's research suggests that the nickname remains in use, although sources disagree about its significance.

---

[83] "Melanie Reid," Duncan School of Law, Lincoln Memorial University, https://www.lmunet.edu/academics/schools/duncan-school-of-law/faculty-staff/faculty/melanie-reid (accessed November 6, 2017); Melanie M. Reid, "NSA and DEA Intelligence Sharing: Why it is Legal and Why Reuters and the Good Wife Got it Wrong," *SMU Law Review*, vol. 68 (2015), p. 465, available at http://scholar.smu.edu/cgi/viewcontent.cgi?article=1029&context=smulr (accessed November 6, 2017).

[84] Burney blog. Human Rights Watch has located a footnote in a 2003 report by the Justice Department's Office of the Inspector General stating, "Title III of the Omnibus Crime Control and Safe Streets Act of 1968 [the Wiretap Act] provided for the use of court-ordered electronic surveillance in the investigation of certain specified violations. The law provided that wiretaps could be used in emergency situations, but if a warrant was not obtained within 48 hours then any information obtained could not be used in court or even revealed." It is unclear why this footnote employs the past tense when describing Title III, and the apparent implication that the government might be able to engage in "emergency" wiretaps under the law without ultimately seeking a warrant if the authorities chose not to "use[]" the information in court is unexplained and remains of interest to Human Rights Watch. The footnote appears following a glossary entry for "Centralized Data Intercept," which is described as "serv[ing] as a central collection and distribution point for the call data information related to Title III." Office of the Inspector General, Department of Justice, "Department Critical Infrastructure Protection Implementing Plans to Protect Cyber-Based Infrastructure," November 2003, https://oig.justice.gov/reports/plus/a0405/app6.htm (accessed November 6, 2017). While the text of Title III provides for emergency wiretaps, the same provision establishes that if the government fails to obtain a valid judicial order within 48 hours, "the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter"—that is, illegally. 18 U.S.C. § 2518(7). Burney's statement and the footnote to the 2003 report suggest that further inquiries in this area are desirable, although Burney's mention of "[w]iretaps" is ambiguous and may refer to an activity under a legal authority other than Title III.

[85] DEA Museum Lecture, p. 14.

[86] Ibid.

"The Dark Side does stuff that doesn't come to the public's attention," the former federal prosecutor who requested anonymity told Human Rights Watch in an interview.[87] This former prosecutor, who claimed to have been part of the Dark Side for a few months, also suggested that the Dark Side included personnel from the CIA, NSA, and Defense Department in addition to the DEA; he characterized the term as referring to a type of activity and not necessarily as a specific, designated unit.[88]

Burney stated in his blog post that when he was interacting with the SOD, he and his coworkers referred to the division as the Dark Side "only half-jokingly."[89]

By contrast, Rizer portrayed the "Dark Side" nickname in his interview with Human Rights Watch as "a tongue-in-cheek kind of thing. When we all left, we got little keychains of Darth Vader."[90] He added that while "there's nothing official called the Dark Side," the entity or activity "is the intersection of the criminal justice system and the intelligence community."[91] (According to Rizer, the SOD also contains a component that is unofficially known as the "Light Side.")[92] Although he declined to provide details about the Dark Side, he emphasized that "[i]t's not as sinister as people think it is," and that "[t]he atmosphere that I saw was painful in ensuring that no laws were violated."[93]

During the same interview, however, Rizer emphasized that the public should think about just how extensive US surveillance powers are. "The powerful aspect of the SOD," he said, "is that they do everything legally—but the laws are so fucking powerful."[94] In other words, the problem is what the laws permit. "The public outcry should really be about the expansive powers of the federal government," Rizer concluded.[95]

---

[87] Human Rights Watch interview with a former US federal prosecutor who requested anonymity, United States, 2016.

[88] Ibid.

[89] Burney blog.

[90] Human Rights Watch interview with Arthur Rizer, Washington, DC, June 8, 2017. Darth Vader is a fictional character from the US science-fiction film series *Star Wars*, and is associated with a sinister type of power famously described in the films as the "dark side."

[91] Human Rights Watch interview with Arthur Rizer, Washington, DC, June 8, 2017.

[92] Ibid.

[93] Ibid.

[94] Ibid.

[95] Ibid.

b. The SOD's role in parallel construction

Sources consistently describe the SOD as distributing tips to other agencies, subject to a mutual understanding that the tips will not be revealed in court proceedings. Typically, the division does not disclose the original source of its knowledge, even to other law enforcement officers or prosecutors. Rizer explained the government's perspective after obtaining and deciding to share information that may be useful in a US criminal investigation: "A lot of times, you don't want the bad guys to know how you got [the] information…. You want to give [law enforcement] just enough" to start an investigation, but "not enough to know where everything came from."[96]

In his blog post, Burney concurred, writing that during his time as a prosecutor:

> It was well understood that you couldn't build a case off of [the SOD's] information. We'd never know where their information came from, for one thing. Without a source to put on the stand, the information couldn't even be a brick in the wall of any case we wanted to construct.
>
> And to be fair, the SOD folks themselves were very clear in their instructions: Their information was not to be used as evidence. It was only to help us figure out what we were looking at in an investigation, and let us know about other things we might want to be looking for. It was all along the lines of "how you gather your evidence is up to you, but you ought to know that this Carlos guy you're looking at is part of a much larger organization, and his role is… and their shipment chain appears to have nodes here, here, and here… and your subject Gilberto over here is looking for a new local dealer."[97]

The former federal prosecutor who requested anonymity indicated to Human Rights Watch that the government has a fundamental dilemma when it is conducting an intelligence operation and, as part of that operation, obtains evidence of a criminal activity (such as a "go-fast" boat that will soon arrive at certain coordinates and may be carrying banned

[96] Ibid.

[97] Burney blog.

substances). "It's a balancing act," he said: the government wants to catch the suspected crime, but does not want to reveal its wiretap or other source.[98]

Maltz was emphatic in his description of the SOD as a law-abiding agency, saying, "SOD is a recognized international law enforcement center for excellence. They try to do the right thing 100 percent of the time."[99] However, as noted elsewhere in this report, the use of parallel construction means executive branch agencies such as the DEA (and its parent agency, the Justice Department) are determining whether many of their own activities are legal—without the checks that judicial review in the course of criminal trials would provide.

B. How Parallel Construction Is Carried Out

The available evidence indicates that the government has a variety of ways of carrying out parallel construction.

1. Call records

As noted above, law enforcement agents in the US may obtain records of telephone calls (although not the content of the conversations) without a warrant. An entry in an IRS manual that was reportedly available to personnel from 2005 to 2007 indicates that parallel construction methods may include—among others—subpoenas of domestic telephone call records or requests for foreign call records or subscriber information.[100]

In 2013, reports emerged that the DEA had been gaining access to enormous volumes of call records from the US telecommunications company AT&T through a program known as Hemisphere.[101] A government presentation indicated that agents could issue subpoenas to re-obtain any call records they originally found through Hemisphere, thus preventing the program from being disclosed—an apparent form of parallel construction.[102] The American

---

[98] Human Rights Watch interview with a former US federal prosecutor who requested anonymity, United States, 2016.

[99] Human Rights Watch telephone interview with Derek S. Maltz, August 3, 2017.

[100] Shiffman and Ingram.

[101] Scott Shane and Colin Moynihan, "Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s," *New York Times*, September 1, 2013, http://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html (accessed November 6, 2017).

[102] "Los Angeles Hemisphere," *New York Times*, undated, p. 10, http://www.nytimes.com/interactive/2013/09/02/us/hemisphere-project.html (accessed October 20, 2017).

Civil Liberties Union and the Electronic Frontier foundation have argued in court that Hemisphere is unconstitutional.[103]

An investigation by the Justice Department's Office of the Inspector General regarding "the DEA's use of administrative subpoenas to obtain broad collections of data or information," including "the use of 'parallel construction' or other techniques to protect the confidentiality of these programs," remained ongoing the time of writing.[104]

2. Interviews and searches based on consent

In some circumstances, the government may engage in parallel construction by eliciting information directly from suspects or asking them for consent to perform a search. The IRS manual entry mentioned above refers to "[f]ield interviews/defendant debriefs" as a parallel construction technique.[105] Meanwhile, a federal case in New Mexico, *United States v. Grobstein*, highlights the potential use of consent searches: based on security videos recorded at the Albuquerque bus station, defense attorneys alleged that a DEA agent secretly (and unlawfully) searched luggage left on a long-distance bus during a layover, then—after the passengers had re-boarded—approached the defendant seeking consent to search his bag.[106]

Pretextual traffic stops, discussed below, may also lead to attempts by officers to obtain consent to perform a search.

3. Intelligence surveillance

It is also possible that the government is using some forms of intelligence surveillance to hide other forms of such surveillance. For example, as explained above, the government has previously given defendants notification of individualized orders under longstanding and relatively uncontroversial provisions of FISA while avoiding disclosing its use of more

---

[103] *United States v. Diaz-Rivera*, case no. 12-cr-00030 (N.D. Cal.), Brief of *Amici Curiae* of ACLU, ACLU of Northern California and Electronic Frontier Foundation in Support of Defendants' Motion to Compel Discovery, filed October 15, 2013, https://www.aclu.org/files/assets/usvdiazrivera-amici_curiae_brief_of_aclu_aclunc_eff.pdf (accessed December 21, 2017).

[104] Office of the Inspector General, Department of Justice, "Drug Enforcement Administration: Ongoing Work," undated, https://oig.justice.gov/ongoing/dea.htm (accessed November 7, 2017).

[105] Shiffman and Ingram.

[106] *United States v. Grobstein*.

controversial Section 702 programs. Additionally, DEA training documents obtained by Ciaramella highlight "FISA" (presumably meaning such relatively uncontroversial orders) as a means of enhancing the sharing of information between the Intelligence Community and law enforcement.[107]

Even the government's secretive surveillance under Section 702, when disclosed, might serve to conceal other intelligence surveillance sources. A defendant who received notice of Section 702 surveillance in 2015 went on to ask for the disclosure of any monitoring pursuant to two other intelligence authorities, Executive Order 12333 and national security letters; the prosecution responded that he was not entitled to any such notification.[108] This raises the prospect that the government may be using intelligence surveillance methods to conceal other, even more secretive intelligence surveillance methods.

4. Proceedings under the Classified Information Procedures Act

Adopted in 1980, the Classified Information Procedures Act ("CIPA") creates procedures for the treatment of classified information that a party to a case in the US—including the prosecution or a criminal defendant—may wish to introduce into evidence. To resolve such matters, the law enables the court to take actions such as holding pretrial hearings, issuing protective orders, and directing the government to provide the defendant with a redacted copy or declassified summary of classified evidence.[109]

Arthur Rizer, the former federal prosecutor who worked at the SOD from 2010 to 2013, suggested in his interview with Human Rights Watch that CIPA "is a very misunderstood, incredibly powerful statute" and pointed out that it allows prosecutors to "sanitize discovery" of classified information.[110] The implications of Rizer's statement for parallel construction currently remain unclear; however, CIPA features prominently in several places in the DEA training documents obtained by journalist Ciaramella. For example, one of these documents states that CIPA (and FISA) "provide a means lawfully to limit exposure

---

[107] Muckrock documents, p. 71 of the complete PDF.

[108] *United States v. Mohammad*, case no. 3:15-cr-00358 (N.D. OH), Government's Response in Opposition to Defendant's Motion for Notice and Additional Discovery Regarding Surveillance Techniques (doc. 137), filed September 13, 2016, pp. 12-13.

[109] See Classified Information Procedures Act, 18 U.S.C. App. §§ 1 et seq.

[110] Human Rights Watch interview with Arthur Rizer, Washington, DC, June 8, 2017.

of sensitive information during public trials" and that "the concept known as 'parallel construction' can be used to shield classified information that might otherwise be discoverable in a trial from the discovery process at trial by using the [CIPA] and a 'Taint Review Team.'"[111]

5. Pretextual traffic stops

At least in the area of narcotics enforcement, one of the best documented parallel construction techniques is pretextual traffic stops. The documents Ciaramella obtained indicate that the use of "[a] wall off or pretext stop" is an accepted tactic.[112] Human Rights Watch has also identified numerous federal and state judicial decisions in which the government has admitted, after the fact, to having carried out what are known as "whisper," "wall," "walled off," or "wall off" stops.[113] It is unclear how the government decides whether to disclose the fact a traffic stop was pretextual on its own initiative during proceedings: in at least one case 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).[114] In another case 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.[115]

In a 2014 Sixth Circuit judgment vacating a defendant's guilty plea due to an unlawful frisk (that is, pat-down of an individual) following a "wall off" stop, the court summarized the nature of these stops: "During an undercover investigation, if it is necessary to stop a suspect's vehicle, law enforcement will sometimes request that a marked patrol car

---

[111] Muckrock documents, pp. 96, 117; see also p. 71.

[112] Muckrock documents, p. 203 of the complete PDF.

[113] E.g., *United States v. Son*; *United States v. Munoz*; *United States v. Norton*, 2016 U.S. Dist. LEXIS 69177 (N.D. IN), April 28, 2016; *United States v. Bateman*, 2009 U.S. Dist. LEXIS 56259 (E.D. TX), June 25, 2009.

[114] *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; Human Rights Watch interview with a former federal prosecutor who requested anonymity, 2016 (suggesting that the defense cannot count on prosecutors coming forward with this information in "wall stop" cases and calling on defense attorneys skeptical about the reasons for traffic stops to directly challenge the government with questions such as "'Why were you [law enforcement] in that position? Who told you to go there?'").

[115] *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.

initiate a traffic stop based on a traffic infraction in order to avoid disclosing the larger investigation's existence."[116] Similarly, a 2012 Eleventh Circuit decision concerning a case involving an ICE request for a traffic stop in order to protect a "confidential source" described "whisper stops" as ones in which the government "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."[117]

A detective testifying in a 2005 federal case in Utah explained even more bluntly that during a "walled-off" stop, "We will use patrol vehicles to initiate stops for offenses other than what we are doing our investigation on. And then, of course, we are expecting or hoping that there would be something more coming out of that traffic stop, such as the seizure of narcotics or weapons, etcetera. Basically what we're doing is we're trying to build a wall between what's happening with our investigation and the suspect at the time."[118]

The earliest published court opinions located by Human Rights Watch describing what may have been pretextual stops for parallel construction purposes describe stops requested in Indiana and Illinois in 1985.[119] Over time, such cases appear to have become far less unusual: using search terms such as "wall stop" and "whisper stop," Human Rights Watch has located dozens of published opinions indicating that such stops had been performed. For several reasons, these cases may represent a fraction of the actual total: not all opinions are published or otherwise included in databases, many defendants in the US accept plea bargains at early stages of their cases (such that courts never write opinions resolving legal issues), and there is no indication that the government believes it is legally obligated to inform defendants that a traffic stop was pretextual.

In an interview with Human Rights Watch, Rizer stated that a tip to law enforcement for parallel-construction purposes might be "as simple as, 'Look for a white car at this intersection at this time.'"[120] In his blog post, Burney wrote:

---

[116] *United States v. Noble*, 762 F.3d 509, fn. 1 (6th Cir. 2014).

[117] United States v. Sanders, p. 1303.

[118] *United States v. Cervantes*, 2005 U.S. Dist. LEXIS 34870 (D. Utah 2005), p. 3.

[119] *United States v. Rodriguez*, 831 F.2d 162 (7th Cir. 1987); *United States v. Celio*, 945 F.2d 180 (7th Cir. 1991).

[120] Human Rights Watch interview with Arthur Rizer, Washington, DC, June 8, 2017.

> [L]et's say you know that a blue van with Florida plates XXX-XXXX will be going up I-95 this weekend, loaded with heroin in a variety of clever traps. But you can't just pull it over because you can't introduce that information in court for whatever reason. Instead, you follow it in a series of unmarked cars, until it makes a moving violation. Which is very likely to happen, no matter how careful the driver is (it's practically impossible to travel very far without committing some moving violation or other). You now have a lawful basis to pull the van over. And a dog sniff doesn't even count as a Fourth Amendment search, so out comes the convenient K-9. And tada! Instant lawful search and seizure, and the original reason why you were following him is not only unnecessary but irrelevant.[121]

Similarly, the first Reuters article on parallel construction quotes a "former federal agent in the northeastern United States" as saying, "You'd be told only, 'Be at a certain truck stop at a certain time and look for a certain vehicle.' And so we'd alert the state police to find an excuse to stop the vehicle, and then have a drug dog search it."[122]

Court decisions located by Human Rights Watch confirm these accounts of how traffic stops conducted to facilitate parallel construction often unfold. First, an official involved in a related investigation contacts a state or local law enforcement officer with a request that a vehicle matching a certain description be stopped.[123] In some instances, although not all,[124] the official requesting the stop does not provide any further information about the underlying investigation or any drugs or contraband he or she believes the vehicle may be carrying.[125] The officer conducting the stop is expected to find an independent reason for doing so—typically, a violation of traffic laws.[126] (Examples of such violations in past cases have included speeding, failing to signal a lane change, weaving over a line demarcating a

[121] Burney blog.

[122] Shiffman and Cooke.

[123] E.g., *United States v. Munoz*.

[124] E.g., *United States v. Alonzo*, 2016 U.S. Dist. LEXIS 51043 (D. Minn.), April 15, 2016; *United States v. Son*, Order, October 2, 2012, https://www.leagle.com/decision/infdco20121004a91 (accessed December 14, 2017).

[125] E.g., *United States v. Munoz*; *United States v. Covarrubias*, 2007 U.S. Dist. LEXIS 199 (D. Or.), January 4, 2007; *United States v. Cervantes*; *United States v. Marquez-Martinez*, 2009 U.S. Dist. LEXIS 6961 (D. Kan.), January 30, 2009.

[126] E.g., *United States v. Gonzales*, 121 F. Supp. 3d 1094 (D. NM 2015); *United States v. Munoz*; *United States v. Son*.

lane, and having improperly tinted windows.[127]) In one Ninth Circuit case in which the court upheld the validity of the stop, no traffic violation actually occurred, although officers falsely told the driver they had observed one.[128] In another case, a federal court upheld the validity of the pretextual stop and search of a vehicle for drugs even though the officer knew the government had already removed the narcotics for which he was ostensibly searching and had replaced them with a "sham" substance—in other words, he knew that there would be no drugs.[129]

After stopping the vehicle, the officer may ask for consent to search it.[130] If the driver does not provide such consent, the officer may arrange for a drug-detecting dog to sniff the vehicle.[131] Depending on the circumstances, the officer may "frisk" (that is, pat down) the driver and/or passengers.[132] In some cases, an officer who has not found any evidence of contraband may tell the driver that he or she is free to go, then begin a "consensual conversation" with him or her or request to ask some additional questions—the answers to which may give the officer legally sufficient reason to search the vehicle without consent.[133] In one extreme case, the government staged a traffic accident followed by the purported theft of the defendant's car and a high-speed chase; in 2007, the Ninth Circuit ruled that this "ruse," which was intended to conceal DEA surveillance, was legal.[134]

Rizer and the other former federal prosecutor interviewed by Human Rights Watch confirmed that the issuance to local law enforcement of "Be On the Lookout Orders," or BOLOs, are one means by which agencies might prompt such traffic stops in order to avoid

---

[127] *Fertig v. Wyoming*, 146 P. 3d 492 (Wyo. S. Ct.), November 17, 2006; *United States v. Bateman*; *United States v. Son*, Order; *Commonwealth v. Young*, 2015 Pa. Dist. & Cnty. Dec. LEXIS 38, March 12, 2015.

[128] *United States v. Magallon-Lopez*, 817 F.3d 671 (9th Cir. 2016); see also *United States v. Chavez*, 534 F.3d 1338 (10th Cir. 2008) (upholding the validity of a wall stop although the supposed traffic violation identified by the officer did not in fact constitute a violation of the law).

[129] *United States v. Son*, Order.

[130] E.g., ibid.

[131] E.g., ibid.; *United States v. Reidy*, 2013 U.S. Dist. LEXIS 151493 (D. Mont.), October 8, 2013.

[132] E.g., *United States v. Noble*.

[133] E.g., *United States v. Pickel*, 2014 U.S. Dist. LEXIS 53530 (D. Kan.), April 2, 2014; *United States v. Sanchez-Tamayo*, 2011 U.S. Dist. LEXIS 154851 (N.D. Ga.), November 28, 2011; *United States v. Evans*, 786 F.3d 779 (9th Cir. 2015); *United States v. Chavez*.

[134] *United States v. Alverez-Tejeda*, 491 F.3d 1013 (9th Cir. 2007).

disclosing the fact that information was obtained from certain sources.[135] Examples of BOLOs appear in emails disclosed to WikiLeaks that belonged to Stratfor, a private Texas-based intelligence firm. After describing vehicles that the sender of the BOLO believes may be involved in narcotics trafficking or other unlawful activities, several of these documents explicitly instruct law enforcement to "[d]evelop your own probable cause for conducting a traffic stop."[136] (It is unknown whether any of the specific BOLOs located by Human Rights Watch were issued based on intelligence activities, although the instruction to "develop your own probable cause" indicates that the government did not initially plan to disclose the original source of its information to the defendant.)

Overall, Rizer suggested that 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."[137]

Courts across the nation have accepted this practice of pretextual traffic stops, if at times reluctantly. As noted above, the US Supreme Court's decision in *Whren* established for the purposes of US constitutional law that an officer may stop a driver whenever the officer objectively has sufficient reason to believe the driver has committed a traffic violation—regardless of whether the officer has some other motive for carrying out the stop.

The transcript of the cross-examination of a state trooper by a defense attorney in a Georgia case illustrates how this rule facilitates parallel construction:

> Q. So you called this a whisper stop, correct?

---

[135] Human Rights Watch interview with Arthur Rizer, Washington, DC, June 8, 2017; Human Rights Watch interview with a former US federal prosecutor who requested anonymity, United States, 2016.

[136] These BOLOs from the leaked Stratfor emails may be viewed at the following links:
https://wikileaks.org/gifiles/docs/28/2870237_corrected-bolo-suspected-meth-smuggler-mexico-to-atlanta-ga-.html;
https://wikileaks.org/gifiles/docs/28/2890348_fw-bolo-possible-narcotics-smuggling-.html;
https://wikileaks.org/gifiles/docs/29/2942193_fw-possible-narcotics-currency-trafficker-contact-sa-steven.html;
https://wikileaks.org/gifiles/docs/28/2833293_fw-bolo-narcotics-smuggling-white-denali-.html;
https://wikileaks.org/gifiles/attach/136/136917_BOLO-Possible%20Narcotics%20Smuggling.pdf;
https://wikileaks.org/gifiles/docs/28/2833019_bolo-possible-drug-smuggler-.html;
https://wikileaks.org/gifiles/attach/136/136844_2012-0086%20BOLO.pdf;
https://wikileaks.org/gifiles/docs/28/2886801_possible-alien-smuggling-in-ept-aor-.html; and
https://wikileaks.org/gifiles/docs/29/2943328_-alpha-insight-cbsa-2-aric-ag-3-cfix-ciac-2-and-dhs.html (last file listed at end of message); (all accessed November 6, 2017).

[137] Human Rights Watch interview with Arthur Rizer, Washington, DC, June 8, 2017.

A. That's correct.

Q. I guess that is a term you guys use in your job?

A. That's correct.

Q. It is really a ruse, isn't it? I mean, you are trying to protect an informant's identity, that is your testimony, right?

A. That's right.

Q. You are trying to make the driver… think you are stopping him for some other reason, but that is really a ruse, isn't it?

A. The reason I stopped him was a valid reason. The reason I did what I did was to protect the identity of the confidential informant so the target would believe that I was stopping him for a traffic violation and not that he was burnt.

Q. So you were sort of pretending and you knew exactly what you were looking for when you pulled the car over, right?

A. Right.

Q. You are pretending, but you don't want the driver to know what is going on?

A. To protect the identity of the confidential informant.

THE COURT: The answer is yes, you don't want the driver to know.

THE WITNESS: Yes, correct, yes, ma'am.

> THE COURT: Yes, Mr. Finlayson, you know under Supreme Court law it makes no difference, so move on.[138]

After the stop has occurred, other US Supreme Court decisions allow officers to conduct canine sniffs without a warrant, although they cannot unreasonably prolong the stop to do so in the absence of probable cause to believe an offense has occurred.[139] However, an increasingly prevalent doctrine of "collective knowledge" that has emerged among the lower courts means many judges continue to take an expansive view of when an officer has reasonable suspicion to prolong the traffic stop beyond the time that would have been required to address the traffic violation.[140] Also known as the "fellow officer" rule, the doctrine treats knowledge possessed by one law enforcement officer (such as a DEA agent) as also being possessed by others involved in the investigation (such as the state or local officer conducting the traffic stop), even if those other officers do not know the relevant facts. As a result, some courts have held that an action taken by law enforcement during a traffic stop was based on a reasonable suspicion or probable cause (as applicable), even though the action in question would otherwise have been unconstitutional due to a lack of sufficient fact-based suspicion on the part of the officer who actually carried out the stop.[141]

Some courts have begun to express discomfort with the consequences of the permissive doctrines that have developed in relation to wall stops and other traffic stops—but believe they have no choice but to apply them. Most strikingly, Judge Marsha Berzon of the Ninth Circuit expressed frustration in a concurrence with a ruling that a traffic stop was valid even though the officer conducting the stop lied to the driver when claiming that a traffic violation had occurred. "Is it fine for police officers flatly to tell the drivers they stop that they observed—or thought they observed—a traffic violation when they really did not? We hold today that it is," she wrote, suggesting that precedents such as *Whren* left the court with no choice. These precedents, she suggested, "are especially troubling in that they enable artifice and abuse by law enforcement, with disproportionate effect on racial

---

[138] *United States v. Son*, pp. 39-40.

[139] *Illinois v. Caballes*; *Rodriguez v. United States*, 575 U.S. __ (2015).

[140] See, e.g., *United States v. Jensen*, 425 F.3d 698 (9th Cir. 2005); *United States v. Chavez*.

[141] E.g., *United States v. Alonzo*; *United States v. Marquez-Martinez*.

minorities."[142] Judge Frances Tydingco-Gatewood, chief judge of the federal district court of Guam, similarly expressed concern about the requirements imposed by precedent when applying the collective knowledge doctrine to a wall stop. While upholding the validity of such a stop based on collective knowledge, her opinion acknowledged that the decision "stretche[d] the confines of the Fourth Amendment" and indicated that "the lack of candor and inconsistent position of many of the United States' witnesses" had been "deeply disturbing."[143]

C. Frequency of Parallel Construction

Human Rights Watch has received conflicting information about the frequency of parallel construction.

For example, Robert Litt, a former general counsel of ODNI, told Human Rights Watch in response to a question about how often parallel construction occurs, "It is not the routine practice in criminal cases. I'm quite confident that it is a small minority of the overall realm of criminal cases in which it's used."[144] Regarding intelligence information specifically, the DEA documents obtained by Ciaramella state that "highly classified [Intelligence Community] information is being used to assist [law enforcement agents] in their investigative activities," but that this is "not the normal course of business."[145]

By contrast, Reuters has quoted an anonymous senior DEA official as saying, "Parallel construction is a law enforcement technique we use every day."[146] Rizer told Human Rights Watch that when he was part of the SOD, there were "thousands of sealed indictments around the country involving the kind of work the SOD was doing" and that the use of SOD tips for US prosecutions "was a daily affair."[147] He added that this "tip and lead" practice

---

[142] *United States v. Magallon-Lopez*, pp. 676-77 (Berzon, J., concurring). Judge Berzon may have been alluding to concerns that racial minorities in the United States are disproportionately subjected to traffic stops and citations. For a discussion of this topic, see Sharon LaFraniere and Andrew W. Lehren, "The Disproportionate Risks of Driving While Black," *New York Times*, October 24, 2015, https://www.nytimes.com/2015/10/25/us/racial-disparity-traffic-stops-driving-black.html (accessed November 7, 2017).

[143] *United States v. Martinez*, 2016 U.S. Dist. LEXIS 147543 (D. Guam 2016).

[144] Human Rights Watch telephone interview with Robert Litt, former General Counsel of the Office of the Director of National Intelligence, August 29, 2017.

[145] Muckrock documents, p. 33 of the complete PDF.

[146] Shiffman and Cooke.

[147] Human Rights Watch interview with Arthur Rizer, Washington, DC, June 8, 2017.

was done "across DOJ," and not only at the SOD.[148] Joseph O'Keefe, a former special-agent-in-charge of the SOD, said during the 2015 DEA panel, "I think every day there's cases that are affected by products that come out to the field through SOD from the Fusion Center that multi-jurisdiction operations go on" (although he did not specify the nature of these products or the role of the fusion center).[149]

Thus, while the frequency with which the government uses parallel construction to conceal intelligence surveillance or other intelligence activities remains unclear, it may be common. In particular, sources suggest that information from the DEA's SOD regularly leads to or forms part of investigations and prosecutions nationwide, although the division's role does not appear to be disclosed routinely (if ever) in criminal cases. More broadly, the evidence suggests that the use of parallel construction to conceal some type of investigative source (intelligence-related or otherwise) from defendants, at least during the initial stages of an arrest and prosecution, is widespread.

D. Who Is Affected by Parallel Construction

Many of the government-acknowledged "wall stop" cases located by Human Rights Watch through searches of published opinions resulted in prosecutions of defendants for trafficking significant amounts of drugs. However, a few suggested that law enforcement may be deploying the technique in more minor cases. For example, in a Louisiana state case, a DEA tip led to the wall stop of a suspect who was found to be carrying approximately five pounds of marijuana and was ultimately charged with a single count of possession with intent to distribute.[150] A Wyoming state case involving the use of an avowedly "pretextual" traffic stop for speeding resulted in the prosecution of a man who was found to be carrying contraband suggestive of personal drug use, including a "kitchen spoon" that had apparently been "used to heat powdered methamphetamine into a liquid for intravenous injection," along with ten grams of methamphetamine.[151]

---

[148] Ibid.

[149] DEA Museum Lecture, p. 34. "Fusion centers" are federally funded entities that promote information-sharing between federal, state, and local authorities. Carrie Johnson, "Report Slams Counterterrorism 'Fusion Centers'," National Public Radio, October 3, 2012, https://www.npr.org/2012/10/03/162246652/report-slams-counterterrorism-fusion-centers (accessed December 13, 2017). The transcript suggests that O'Keefe was referring to a specific fusion center.

[150] *State v. Meyers*, 100 So. 3d 938 (La. App. 2012).

[151] *Fertig v. State*, 146 P.3d 492 (S. Ct. Wyo. 2006). In a 2016 report, Human Rights Watch and the American Civil Liberties Union called for addressing drug possession for personal use through a public health approach and for the decriminalization

The government may also be deploying parallel construction techniques other than traffic stops against relatively low-level offenders. In 2015, *USA Today* reported that police in Baltimore had used cell-site simulators to investigate crimes such as harassment, cell phone and automobile theft. According to the report, the use of the devices in these cases had previously been undisclosed.[152]

E. The Government's Legal Justifications for Parallel Construction

While the government has not explicitly revealed its theory as to why it believes parallel construction to be legal under US law, evidence suggests the theory is based on government lawyers' interpretations of cases relating to the "fruit of the poisonous tree" doctrine described above. In other words, the government may be concealing certain investigative activities based on its own determination that its later efforts to relocate the same or related information qualify as independent or sufficiently attenuated from the original activity to avoid the risk of taint from any unlawful conduct (or that officials inevitably would have discovered the same information even without the potentially unlawful behavior).

This understanding of the government's approach is supported by information submitted by Director of National Intelligence Dan Coats to a committee of the House of Representatives in July 2017. Coats indicated that where the use of data from a Section 702 surveillance program is concerned, the government's standard for determining whether evidence in a case is "derived from" Section 702 (thus legally entitling the defendant to specific notice of this surveillance) "incorporates a 'fruit of the poisonous tree' analysis analogous to that conducted under the Fourth Amendment exclusionary rule context."[153] Coats went on to refer to the independent-source, inevitable-discovery, and attenuation exceptions to the "fruit of the poisonous tree" doctrine.[154]

---

of the possession of drugs for personal use due to the excessive sentences and related human rights problems that ensue during prosecution and conviction. Human Rights Watch, *Every 25 Seconds* (New York: Human Rights Watch, 2016), https://www.hrw.org/report/2016/10/12/every-25-seconds/human-toll-criminalizing-drug-use-united-states.

[152] Heath, "Police secretly track cell phones to solve routine crimes."

[153] Letter from Daniel R. Coats to Bob Goodlatte and John Conyers, Jr., July 17, 2017, p. 18, https://www.documentcloud.org/documents/4320685-SSCI-ODNI-FISA-702-QFRs-2017-06-07.html#document/p11/a390936 (accessed December 10, 2017).

[154] Ibid.

"Under US law, a defendant has the right to challenge the evidence used against him or her in court—whether it derived directly or indirectly from unlawful activity," Robert Litt, the former general counsel of ODNI, explained in correspondence with Human Rights Watch about parallel construction.[155] "However, there is a whole host of case law delineating when evidence is and is not derived from unlawful activity (fruit of the poisonous tree), and," he wrote, "a defendant doesn't have the right to challenge government activity that didn't lead to evidence under those cases, save for an argument like entrapment."[156] Current officials may be embracing a logical extension of views like Litt's as an internal justification for refraining from disclosing evidence to the defense if it believes the defendant would not have a right to challenge the underlying government activities.

When discussing parallel construction with Human Rights Watch, Litt also mentioned a decades-old Supreme Court decision in *Roviaro v. United States*, a case in which the court accepted that it may be constitutional for the government to conceal the identity of a human informant from a defendant in some circumstances.[157] The DEA documents obtained by journalist Ciaramella highlight *Scher v. United States*, in which the Supreme Court issued a similar holding.[158]

Whatever the government's internal justifications for deliberately concealing a source of information (such as a surveillance program) may be, the use of parallel construction means judges are deprived of their role in applying this prior case law—the Supreme Court's holdings and any subsequent federal court decisions, as well as relevant state law—to the facts of the case before them. Defendants are also deprived of the opportunity to make counterarguments. Thus, the government secretly places itself in the judge's role, jeopardizing both the fairness of the case at hand and the rights of other individuals affected by official activities that may violate US law or human rights.

---

[155] Email correspondence between Robert Litt, former general counsel of the Office of the Director of National Intelligence, and Human Rights Watch, November 10, 2017.

[156] Ibid.

[157] Human Rights Watch telephone interview with Robert Litt, former general counsel of the Office of the Director of National Intelligence, August 29, 2017.; *Roviaro v. United States*, 353 U.S. 53 (1957).

[158] Muckrock documents, pp. 30, 63, 70, 85, 112, 126, and 156 of the complete PDF; *Scher v. United States*, 305 U.S. 251 (1938).

III. Defendants' Difficulties in Discovering and Challenging Parallel Construction

In some cases, the government has acknowledged in court proceedings that officers conducted a pretextual traffic stop to prevent suspects from realizing at initial stages that information had been obtained from a particular source. In other cases, however, defense attorneys who have suspected that the government has employed some form of parallel construction to conceal an investigative technique have struggled to compel the prosecution to disclose whether this had in fact occurred; this is especially true where the attorneys argue that an intelligence source may have been involved.

Human Rights Watch's research suggests that except in cases where the government—acting on its own initiative—chooses to reveal that it has engaged in parallel construction, defendants currently face a low likelihood of being able to find out whether officials have sought to create a "firebreak in the evidentiary trail."[159]

A. Prosecution Resistance to Defense Motions

Our review of relevant court documents indicates that when defendants make motions to find out whether the government has concealed the true origins of information in their cases, the prosecution rarely answers in a straightforward manner. Instead, prosecutors deploy arguments that prevent defendants from learning definitively whether intelligence or other undisclosed information or sources were used in the investigation.

1. Arguing that the defendant is merely speculating

In several cases Human Rights Watch examined, the prosecution described the defendant's efforts to question whether undisclosed sources or information may have been used in his or her case as "speculation" or a "fishing expedition"—without ever providing a definitive "yes" or "no." This places the burden of justifying the question on the defense attorneys, who are unlikely to be able to validate even reasonable suspicions that secret activities lie behind the investigation of their client. While this response may be

[159] See n. 47 above and accompanying quoted text.

a common one to defense motions in criminal cases, it takes on a particular significance in light of reports that government agencies may intentionally avoid telling prosecutors that they engaged in sensitive investigative techniques[160], as well as the clear difficulties defendants face in obtaining and offering any evidence about classified programs or other activities the government has deliberately sought to conceal.

In *United States v. Syed Ali*, for example, the attorney for a Texas defendant who was accused of selling synthetic marijuana at his smoke shop pointed out in a motion that "[t]he government has provided voluminous discovery [i.e., evidence] in this case, but none that illuminates how the investigation began."[161] The attorney suspected that the government had relied on undisclosed FISA surveillance, since the FBI had originally included the defendant in an investigation related to a suspected terrorism offense (something with which he was never charged) and since one of his co-defendants had communicated with people abroad.[162] Without directly affirming or denying that such surveillance had taken place, the prosecution described the attorney's request as "an impermissible speculative fishing expedition."[163]

Very similar language—and the same lack of an explicit affirmation or denial—has appeared in prosecution responses in several other federal cases around the country.[164] While to some extent this wording is based on prior US judicial decisions[165], it also appears to reflect a consistent tactical choice by prosecutors to avoid having to find out or disclose

[160] Shiffman and Cooke; Brad Heath, "FBI warned agents not to share tech secrets with prosecutors," *USA Today,* April 20, 2016, https://www.usatoday.com/story/news/2016/04/20/fbi-memos-surveillance-secrecy/83280968/ (accessed December 13, 2017).

[161] *United States v. Syed Ali*, case no. 5:13-cr-00580 (S.D. TX), Complaint (doc. 1), filed June 26, 2013, para. 27; Motion for Discovery (doc. 374), filed February 3, 2014, p. 1.

[162] Ibid. at pp. 13-14.

[163] *United States v. Syed Ali*, Government's Response to Defendant's Motion for Discovery (doc. 394), filed February 18, 2014, p. 2.

[164] E.g., *United States v. Alexander*, case no. 1:11-cr-00148 (E.D. IL), Government's Consolidated Response to Defendant's Motion for Discovery of Electronic Surveillance and Special Operations Division Materials (doc. 136), October 4, 2013, p. 2; *United States v. Simmons*, case no. 6:13-cr-06025 (W.D. NY), Government's Memorandum in Opposition to Pre-trial Motions by Tyshawn Simmons (doc. 288), February 25, 2014, p. 24; *United States v. Collins*, case no. 1:13-cr-00383 (E.D. VA), Government's Opposition to Defendant's Motion to Enforce Order Compelling Discovery (doc. 378), September 2, 2014, pp. 1, 5; *United States v. Vawter*, case no. 6:13-cr-03123 (W.D. Mo., United States Response to Vawter's Motion to Compel Discovery (doc. 104), filed April 16, 2015, pp. 7-9.

[165] E.g., *United States v. Mayes*, 917 F.2d 457 (10th Cir. 1990).

whether intelligence surveillance or other previously undisclosed methods were employed in an investigation.

Prosecutors sometimes argue that the *defense* should be required to produce factual materials to support efforts to uncover any parallel construction to lift its inquiry beyond the realm of "speculation." For example, in *Ali,* the prosecution argued that "[t]he defendant does not offer a scintilla of evidence that these FISA intercepts exist."[166]

Another illustration is *United States v. Collins*, a case stemming from distributed denial of service ("DDoS") attacks staged by the activist network Anonymous. Prosecutors noted that a defendant "sought to compel the Government to produce information from the intelligence community allegedly related to this case that he claimed could possibly exist. However, neither in his written motion nor in the oral argument … did the Defendant establish that this information did in fact exist."[167]

Defendants have sometimes sought to reply to these arguments by highlighting circumstances or evidence suggesting that their concerns are more than merely speculative. For example, Jessica Carmichael, one of the defense attorneys in *Collins*, referred to NSA documents leaked by Snowden referring to operations against Anonymous.[168] In *Ali*, the defense attorney noted that his client had initially been the subject of a terrorism investigation.[169]

A more fundamental problem is that even where the defense has reason to suspect intelligence surveillance lies behind a case, the classified nature of these activities leaves no choice but to guess. Then-federal public defender Todd Watson explained in a hearing in *Collins* that while the defense possessed leaked information suggesting that one of the NSA's known intelligence-sharing partners had taken a direct interest in Anonymous, any further information "presumably … is all top secret. Right?" He concluded, "The only way

---

166 *United States v. Syed Ali*, doc. 394, p. 8.

167 *United States v. Collins*, Indictment (doc. 1), October 3, 2013; doc. 378, p. 1.

168 *United States v. Collins*, Motions Hearing (Transcript) (doc. 246), May 12, 2014, pp. 14, 16; regarding the Snowden documents, see "Exclusive: Snowden Docs Show UK Spies Attacked Anonymous, Hackers," *NBC News*, February 5, 2014, https://www.nbcnews.com/feature/edward-snowden-interview/exclusive-snowden-docs-show-uk-spies-attacked-anonymous-hackers-n21361.

169 *United States v. Syed Ali*, Motion for Discovery (Transcript) (doc. 408), March 6, 2014, p. 11.

we get this information is if the Court orders a review and requires [the US intelligence] agencies to provide it to us."[170]

In *Ali*, the prosecution suggested that if courts allow defendants to compel prosecutors to check and see whether undisclosed surveillance was involved in an investigation, "every court" could be faced with the burden of uncovering such surveillance, even if it was only distantly involved in an investigation.[171] In an interview with Human Rights Watch, Ali's defense attorney Simon Azar-Farr described this as "one of those 'scare' arguments."[172] He suggested that judges could take the facts of the case into account in deciding whether to order the prosecution to carry out such a check.[173] Carmichael, a defense attorney in *Collins*, similarly suggested that a judge could take into account any unusual circumstances surrounding the origin of a case even if the defense lacks "concrete evidence" that an undisclosed source was involved.[174] She noted that a judge would not necessarily need to order the prosecution to approach every relevant federal agency at once, but could ask it to take the inquiry one step at a time—"Let's ask these five questions first, and then we'll go farther if we need to."[175] During a hearing in *Collins*, defense attorney John Kiyonaga stated: "Every single agency pertinent to this request has offices that are dedicated to nothing but liaison with other government agencies. There are procedures in place for receiving and answering questions, it's simply a matter of directing an inquiry to the pertinent agencies and seeing it responded to."[176]

In an interview with Human Rights Watch, Robert Litt, the former ODNI general counsel, suggested that defendants should at least need to make an "affirmative showing" that intelligence surveillance may have been used in their cases in order to compel the prosecution to check with the intelligence agencies about this (a logic that would presumably extend to other undisclosed sources or methods).[177] Litt expressed a sense

---

[170] *United States v. Collins*, Transcript, pp. 20-21.

[171] *United States v. Syed Ali*, Transcript, p. 31.

[172] Human Rights Watch telephone interview with attorney Simon Azar-Farr, San Antonio, Texas, June 1, 2017.

173 Ibid.

[174] Human Rights Watch telephone interview with defense attorney Jessica Carmichael, Alexandria, Virginia, July 24, 2017.

[175] Ibid.

[176] *United States v. Collins*, Transcript, p. 21.

[177] Human Rights Watch telephone interview with Robert Litt, former general counsel of the Office of the Director of National Intelligence, August 29, 2017.

that "people are frustrated at an inability to use ordinary legal processes to challenge surveillance, and are looking to use the criminal cases as a way of opening the door to overall challenges of surveillance that they're not otherwise able to bring," adding, "I don't think that is an appropriate function of a criminal case. The purpose of a criminal case is to determine the guilt or innocence of a criminal defendant."[178]

By contrast, Carmichael told Human Rights Watch that while "I don't think the defendant needs to know necessarily every detail of the investigatory process," he or she does have a right to know how the case against him or her began.[179] "It's a constitutional principle," she said. "We have the right to challenge evidence that's presented in court," which includes need to be able to challenge any unlawfully gathered evidence.[180]

Azar-Farr told Human Rights Watch:

> It's very straightforward. Every judge in this country knows it, every prosecutor knows it, and either they are too gutless to admit this or to hold the government's feet to the fire…. Every judge should know that when people are gathered and a citizen is accused in his courtroom, the case is not about the judge or the prosecutor or the courtroom deputy or the building itself. It's only about the citizen accused. We're all here, every one of us, in order to ensure that the Constitution is upheld…. You would think that a judge would want to say, "Hey, there is sufficient information in a given case that I now believe that there's a question about this evidence, and before I go forward, I want to make sure that none of this information has come from an intelligence-gathering operation."[181]

In an unusual success for the defense, Judge Liam O'Grady pressed the prosecution in *Collins* to justify its refusal to approach the intelligence agencies, saying:

---

[178] *Ibid.*

[179] Human Rights Watch telephone interview with defense attorney Jessica Carmichael, Alexandria, Virginia, July 24, 2017.

[180] *Ibid.*

[181] Human Rights Watch telephone interview with attorney Simon Azar-Farr, San Antonio, Texas, June 1, 2017.

> [W]hy is it so difficult for the Government to put a lead out to NSA which should, as I understand it, have information from the other intelligence agencies, just to say, was anybody involved in an undercover capacity in these [online] chats during this period of time with this group of defendants concerning these pending [DDoS] attacks?
>
> Why can't you do that? You're acting like this is climbing Mount Everest.[182]

The prosecution agreed to make an initial inquiry with the intelligence agencies about a specific matter, although the case was largely resolved shortly afterward through plea bargains (and the dropping of charges against one defendant).[183]

2. Suggesting that the evidence would not be relevant or discoverable

In some cases, the government has resisted motions for the disclosure of unrevealed investigative techniques by suggesting that any information would not be "relevant" or "discoverable." When making these arguments, it has sometimes relied on its own interpretation of Rule 16 of the Federal Rules of Criminal Procedure. That rule requires it to disclose to the defense "any relevant written or recorded statement by the defendant" that is in its possession (including e-mails or recorded telephone calls, for example), and to allow the inspection of other items within its possession that are "material to preparing the defense."[184]

For example, in *United States v. Daoud*, the prosecution argued in 2013 (quoting prior case law) that it was not required to "divulge every possible shred of evidence that could conceivably benefit the defendant" and that under Rule 16, Daoud needed to be able to

---

[182] *United States v. Collins*, Transcript, pp. 25-26.

[183] The prosecution told the judge: "If Your Honor wants us to ask the intelligence agencies if anybody from the intelligence agencies were in the chat channels that were dedicated by Anonymous in an undercover capacity during the time frame of the conspiracy or involved with any of the victims, the targeted victims, we can do that…" Ibid., p. 26. The hearing was held on May 12, 2014; records available in an online database (Public Access to Court Electronic Records) indicate that much of the substance of the case was resolved through plea bargains between July and October 2014. The indictment of one defendant was fully dismissed on stated grounds related to his disabilities: see *United States v. Collins*, Motion to Dismiss Indictment as to Defendant Phy (doc. 456), filed October 3, 2014.

[184] Federal Rule of Criminal Procedure, no. 16. The DEA training materials obtained by Ciaramella can be read to suggest that relevance is something a trial judge should determine, although it is unclear whether this is the DEA's position in all circumstances. Muckrock documents, pp. 39 and 152 of the complete PDF.

show that the evidence he sought would "significantly alter the quantum of proof in his favor."[185]

In *United States v. Lara*, a federal drug prosecution in California, the defense moved in 2013 for the disclosure of DEA administrative subpoenas that it was concerned might have been used to obtain more types of cell-phone metadata than the government had revealed, or to conceal other surveillance activities.[186] Prosecutor S. Waqar Hasib refused, telling Judge Elizabeth Laporte: "My response is quite simple. We have to draw the line somewhere. We do not have open-file discovery," and "I don't see anything in [the subpoenas] that could conceivably be construed as *Brady* [exculpatory] material. And therefore, I'm not going to turn them over."[187]

Judge Laporte ultimately permitted the prosecution to withhold the subpoenas, saying, "I don't think, so far, there's any showing in this instance" that the government had "hidden the means by which they derived something." However, she added, "I have to say that I wonder."[188] The judge's discomfort with the prospect of parallel construction was clear, even though she characterized the issue as not arising directly in the case before her: "I have to say … I mean, I'm very disturbed by reports that say, you know, get the information one way, and then replicate it, and don't tell the Court how you originally got it. I think that's wrong."[189]

In a striking exchange, the prosecutor then explicitly defended the practice of parallel construction, even where the government has used it to conceal an investigative technique that it knows may be illegal:

> Hasib: I think there are two situations that Your Honor has described. One is where you have an affidavit that's presented to a Magistrate or a District Court Judge, in which a source of information is, in fact, something other than what we purport it to be. That's one situation.

---

[185] *United States v. Daoud*, case no. 12-cr-723 (N.D. IL), Government's Consolidated Response to Defendant's Pretrial Motions (doc. 63), filed August 26, 2013, p. 5.

[186] *United States v. Lara*, Case no. 3:12-cr-00030 (N.D. Cal.), Transcript of Proceedings (doc. 297), Dec. 16, 2013, pp. 31-33.

[187] Ibid. at p. 12.

[188] Ibid. at p. 18.

[189] Ibid. at p. 19.

The Court: Right.

Hasib: That's one situation. And in that situation, I share the Court's concern. That would be a problem.

The other situation, where the Government uses some sort of investigative technique, and then decides to use another investigative technique to re-create what they found the first time—that, I think, is an entirely different scenario.

The Court: It is a different scenario, but it shares some of the same concerns, depending—especially if it were some of the same concerns, depending—especially if it were for the purpose of keeping from the Court something of questionable legality. In other words, it might well be that, you know, you want to protect some informant as much as possible; and you don't want to cite Informant 1; and you'd rather cite Informant 2.

They're both valid sources. There wasn't a contradiction between them, or something like that. That probably wouldn't get you *Brady*.

But if, you know, there was an illegal search, for example, followed by a legal search, but that was only obtained because now that you had the illegal search, you knew something about that, that would be a concern to the Court.

Mr. Hasib: Your Honor, I respectfully –

The Court: And that is the fruit of the poisonous tree, potentially.

Mr. Hasib: I respectfully dispute that point…. I think the second scenario that Your Honor described would be the independent-source doctrine, which I think has been well established in the Supreme Court precedent

> and Ninth Circuit precedent. And that, I think, I have much less concern – in fact, I don't have any concern about that.[190]

In *United States v. Thomas*, a federal terrorism-related case in Pennsylvania, defense attorney Andrew Dalack pointed out to the judge: "The problem, Your Honor, in a nutshell, is this. The Government wants to have it both ways. It wants to be able to on the front end, at the very beginning of an investigation, be able to utilize all of the tools at its disposal"—tools including warrantless intelligence surveillance powers.[191] Referring to government desires to remove limits on information-sharing between law enforcement and intelligence bodies (including a bureaucratic "wall" imposed on the sharing of FISA material prior to the September 11 attacks), he continued:

> The Government wants to be able to essentially not have this wall between foreign intelligence gathering and then gathering of evidence in the course of a criminal prosecution.
>
> But then on the back end, to the detriment of the defendant, Ms. Thomas, the Government wants to resurrect this arbitrary wall between evidence gleaned for strictly foreign intelligence purposes versus evidence gleaned for the purposes of a criminal prosecution.
>
> The Government is not entitled to make arbitrary one-sided, self-serving determinations about whether its evidence is admissible.[192]

3. Maintaining that the evidence is not in the possession of the prosecution team

As noted above, the US Supreme Court established in *Brady v. Maryland* that due process requires the prosecution to disclose evidence that is "favorable" to the defendant.[193] The court later clarified that this obligation includes a "duty to learn" of any such evidence

---

[190] Ibid. at pp. 20-21.

[191] *United States v. Thomas*, case no. 2:15-cr-00171 (E.D. PA), Transcript of Hearing (doc. 75), August 4, 2016, pp. 10-11.

[192] Ibid.

[193] *Brady v. Maryland*.

"known to the others acting on the government's behalf in the case, including the police."[194]

Despite this "duty to learn," in several cases examined by Human Rights Watch, prosecutors resisted defense motions seeking to compel the disclosure of any use of intelligence-derived information in their cases by maintaining that the intelligence agencies were not part of the "prosecution team"; they argued that the prosecution therefore should not be required to make inquiries about those agencies' actions.

For example, in *United States v. Alexander*, a federal drug case in Illinois, the prosecution told the court in 2013 that it had "no reason to believe" any evidence in the case had been obtained from NSA surveillance or SOD leads and insisted that the Supreme Court "has never imposed a responsibility for information not in the government's [meaning the prosecution's] possession, but in the possession of agencies which were not acting on the government's behalf in the case."[195]

Three years later, in a domestic terrorism prosecution arising from the armed occupation of an Oregon wildlife refuge by right-wing activists (*United States v. Bundy*), prosecutors similarly avoided affirming or denying that intelligence-derived evidence had been employed in the investigation, writing that there was "nothing to indicate" that intelligence sources had been used. They added, "Nor have [the] defendants made the showing necessary to require the government to do anything further" under the relevant statute.[196]

In a 2014 motion in *United States v. Simmons*, a federal homicide and drug case in New York, prosecutors stated flatly that "the National Security Agency … is not part of the prosecution team in this case and any information in the NSA's custody or control is, therefore, not subject to disclosure to Simmons under either Brady or Rule 16" of the Federal Rules of Criminal Procedure.[197] The *Simmons* prosecutors used language similar to

---

[194] *Kyles v. Whitley*.

[195] *United States v. Alexander*, case no. 1:11-cr-00148 (E.D. IL), Government's Consolidated Response to Defendant's Motion for Discovery of Electronic Surveillance and Special Operations Division Materials (doc. 136), October 4, 2013, p. 5.

[196] *United States v. Bundy*, case no. 3:16-cr-00051 (D. Or.), Government's Response to Defendants' Motion to Compel Notice of Surveillance and for Production of Related Discovery (doc. 607), filed May 25, 2016, p. 2.

[197] *United States v. Simmons*, case no. 6:13-cr-06025 (W.D. NY), Government's Memorandum in Opposition to Pre-trial Motions of Tyshawn Simmons" (doc. 288), February 25, 2014, pp. 23-24.

what had appeared in *Alexander*, writing that they had "no reason to believe" that evidence had originally come from the NSA.[198]

In *United States v. Khan*, a federal prosecution in Oregon in which the defendant belatedly received notice that Section 702 surveillance had been involved in the case, prosecutors opposed a defense effort to force the government to ensure that any relevant intelligence information not be destroyed. The pertinent discovery rules, they wrote, apply "only to statements, documents, and materials to which federal prosecutors have knowledge and access, that is, generally the files of the Department of Justice and of the investigative agency … Here, the FBI is the appropriate agency."[199] They resisted the possibility that they had an obligation to check with other agencies: "[N]o prosecution, including this one, requires that a defendant be allowed access to all government files, or that other government agencies, not part of the prosecution and investigative team, should be ordered to retain unspecified information not demonstrably material to the defense."[200]

Defense attorneys have responded to such contentions by pointing out their logical weaknesses and the obvious difficulties they create for defendants (who are legally presumed to be innocent).

Defense attorney Jessica Carmichael, who represented a defendant in a prosecution of alleged Anonymous activists (*Collins*), told Human Rights Watch, "The NSA for practical purposes in a general sense may not be part of the prosecution, but if they are providing evidence in a specific case through whatever channels, then they *become* part of the prosecution team."[201] She argued, "You can't not be part of the prosecution team if you're providing evidence to the prosecution," even if the NSA's involvement was far back in the evidentiary chain.[202]

---

[198] Ibid., p. 25.

[199] *United States v. Khan*, case no. 3:12-cr-00659 (D. Or.), Government's Response to Defendant's Motion for Order Directing Government to Preserve FISA/FAA-Obtained Evidence" (doc. 76), May 12, 2014, p. 3.

[200] Ibid., p. 8.

[201] Human Rights Watch telephone interview with Jessica Carmichael, Alexandria, Virginia, July 24, 2017.

[202] Ibid.

In a joint interview with Human Rights Watch, two other attorneys who represented defendants in *Collins* explained the difficulties they had faced. "I wanted to resolve the issue of who [in the government] knew what, when," said John Kiyonaga. "It was simply a matter of telling them to do their jobs."[203]

Fellow attorney Marina Medvin characterized the government's response as "'Our own organization is too big for us to know what's happening.'"[204] She went on to assert, "We don't jail people in America" so that the government can "hide exculpatory evidence for the purposes of national security."[205]

4. Claiming that the government does not intend to "use" evidence as part of the prosecution

One of the most significant controversies concerning intelligence surveillance that has erupted in US courts to date has involved government claims in a challenge to the constitutionality of Section 702 of FISA, *Clapper v. Amnesty International USA*.[206] The case centered on standing: the legal right to bring a case arguing that surveillance is unconstitutional, based on current or future harm. Although the court ruled in the government's favor, the Justice Department issued a policy memorandum stating that "any communications to or from, or information about, a U.S. person acquired under Section 702 of FISA shall not be introduced as evidence against that U.S. person in any criminal proceeding except" in certain types of cases. However, the memorandum did not disclose how the Justice Department decides whether it must notify defendants of Section 702-derived information that it does not formally "introduce[] as evidence"—that is, information it uses in the case in some other way.[207]

---

[203] Human Rights Watch interview with defense attorneys John Kiyonaga and Marina Medvin, Alexandria, Virginia, May 12, 2016.

[204] Ibid.

[205] Ibid.

[206] *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013).

[207] Department of Justice, National Security Division, "Restriction Regarding the Use of FISA Section 702 Information in Criminal Proceedings Against United States Persons," https://www.dni.gov/files/documents/icotr/51117/Doc%2013%20%E2%80%93%20DOJ%20Memorandum%20re%20Restrictions%20on%20the%20Use%20of%20Section%20702%20Information.pdf.

Compounding questions raised by this limited and unclear Section 702-related policy, Human Rights Watch is concerned that in this and other relevant contexts, prosecutors may be adopting restrictive interpretations of when they have "used" surveillance evidence as part of an investigation. For example, in *Thomas*, prosecutors told the court: "The government's decision to use a particular surveillance technique is only discoverable if evidence gathered pursuant to that technique is being used by the government and therefore may be the subject of a defense suppression motion."[208] It is unclear whether prosecutors may have intended to suggest that the defendant was not entitled to learn of any surveillance employed in his case if the government chose not to introduce the resulting data as evidence in court. Similarly, in *Bundy*, prosecutors stated: "If the government had engaged in electronic surveillance or physical searches of the defendants pursuant to FISA *and planned to use evidence obtained or derived from such electronic surveillance* or physical searches *in court* against an aggrieved person as defined under FISA, the government would be under an obligation to notify such aggrieved person."[209]

Of further relevance to this concern is an exchange in *United States v. Sedaghaty*, in which the government charged the defendant with fraud- and customs-related violations and sought to compel a bank to disclose relevant records held in another country. Both the bank and the defendant suggested during a hearing that a US government agency (even if not the prosecution) might already have those records, and the defense indicated that the court should make inquiries accordingly.[210] When responding, the prosecution said, "If we had records that we could use in court at the trial, we wouldn't have gone through" the process of trying to compel the bank to disclose them.[211] Defense attorney Steven Wax, who was then the most senior federal public defender for Oregon, immediately told the judge: "I would point out to you that I found [the prosecutor's] phrasing very, very interesting. If we had records that we could use in court, you know, that doesn't say he doesn't have the records."[212] Subsequent proceedings in the case addressed classified information, although the nature of the information remained undisclosed at the time of writing.[213]

---

[208] *United States v. Thomas*, Case no. 2:15-cr-00171 (EDPA), Government's Response in Opposition to Defendant's Motion for Notice and Discovery of Surveillance Used in the Government's Investigation of the Defendant (doc. 74), July 29, 2016, p. 4.

[209] United States v. Bundy, doc. 607, p. 4.

[210] *United States v. Sedaghaty*, case no. 6:05-cr-60008 (D. Or.), Transcript of Oral Argument (doc. 270), February 16, 2010, pp. 24, 34-35.

[211] Ibid., p. 35.

[212] Ibid., pp. 35-36.

[213] See *United States v. Sedaghaty*, 728 F.3d 885 (9th Cir. 2013).

B. Inadvertent or Politically Motivated Revelations

As noted above, federal government agencies that have sought to employ parallel construction in the form of "wall stops" are sometimes willing to disclose this fact during proceedings, although the government's criteria—if any—for deciding whether to make such disclosures are unclear. In other cases, however, defendants have only learned about previously unrevealed investigative techniques due to carelessness by officials or comments by politicians to whom the government has given classified briefings.

For example, in December 2012 Senator Dianne Feinstein gave a floor speech in support of the renewal of the FISA Amendments Act (which includes Section 702). The speech implied that the government had used intelligence surveillance under the act in its investigations of several defendants who had not previously received any notification from the government to this effect.[214] Among others, these defendants included Mohamed Osman Mohamud, who did not receive a notification of Section 702 surveillance until he had been convicted and was awaiting sentencing.[215]

In January 2015, then-Speaker of the House John Boehner said the government had used "the FISA program" to investigate Ohio defendant Christopher Cornell. The context of the remark suggests that Boehner was referring to Section 702, particularly since he used the case to support the idea that the "program" should be re-authorized.[216] At the time of writing, publicly available court records suggested that the government had not yet disclosed any FISA surveillance to Cornell.

As described above, at least one disclosure of the government's use of a pretextual traffic stop has been inadvertent. The Snowden leaks also gave rise to a challenge by the defendants in *Collins*, and an apparent slip by the government in *Sedaghaty* alerted the defense attorney and judge to the possibility of undisclosed evidence.

---

[214] "FISA Amendments Act Reauthorization Act of 2012," Congressional Record Vol. 158, No. 168 (December 27, 2012), available at https://www.gpo.gov/fdsys/pkg/CREC-2012-12-27/html/CREC-2012-12-27-pt1-PgS8384-2.htm (accessed December 20, 2017).

[215] See *United States v. Mohamud*, 843 F.3d 420, 431 (9th Cir. 2016).

[216] Jake Sherman, "Boehner: Surveillance helped foil alleged plot on Capitol," *Politico*, January 15, 2015, http://www.politico.com/story/2015/01/john-boehner-surveillance-capitol-114294 (accessed October 19, 2017).

These cases prompt concerns that defendants' ability to discover and challenge investigative techniques previously hidden by parallel construction may hinge on the publicity desires of officials or elected representatives, or on serendipity. This, in turn, raises the specter of inconsistent or arbitrary justice.

IV. Impact on Human Rights

Parallel construction may have a serious impact on the human rights of defendants in United States criminal cases—people who are, in line with what human rights require,[217] presumed to be innocent until proven guilty. Additionally, when it is used to conceal surveillance methods, parallel construction deprives the US public—and legislators responsible for enacting laws to govern what law enforcement and intelligence bodies may do—of an understanding of the true extent and impact of secret monitoring. As noted above, by avoiding the potential application of the exclusionary rule, parallel construction also effectively removes one of the most important incentives for law enforcement and other authorities to obey the law.

Under binding international human rights law, proceedings in criminal cases must be "fair" and take place before a "competent" tribunal.[218] Defendants also have a right to "adequate … facilities" for the preparation of their defense, a provision the Human Rights Committee, the UN independent expert committee charged with monitoring compliance with the relevant treaty, has said includes a right of access to "documents and other evidence."[219] According to the committee, "this access must include all materials that the prosecution plans to offer in court against the accused or that are exculpatory," adding that "[e]xculpatory material should be understood as including not only material establishing innocence but also other evidence that could assist the defence."[220]

Furthermore, international human rights law addresses surveillance: all government interferences with privacy (including the privacy of communications) must be necessary to achieve a legitimate aim and must be done in accordance with both international and domestic law—including, in the United States, the Constitution.[221] Any law allowing secret

[217] International Covenant on Civil and Political Rights (ICCPR), adopted December 16, 1966, G.A. Res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, entered into force March 23, 1976, ratified by the United States on June 8, 1992, art. 14(2) (hereinafter "ICCPR").

[218] Ibid., art. 14(1).

[219] Ibid., art. 14(3)(b); Human Rights Committee, General Comment No. 32: "Article 14: Right to equality before courts and tribunals and to a fair trial," U.N. Doc. CCPR/C/GC/32, August 23, 2007.

[220] Ibid.

[221] See ICCPR, art. 17(1).

surveillance must be "sufficiently clear in its terms to give citizens an adequate indication as to the circumstances" in which the monitoring may take place.[222] Human rights law also provides that governments in most circumstances must notify people whose private information has been surveilled.[223]

If an individual's fair-trial, privacy, or other rights are violated, human rights further require that he or she must receive an effective remedy.[224]

Parallel construction violates, or facilitates violations of, each of these rights. A defendant who is unable to discover and challenge the use of an investigative source or method that was employed in his or her case and that may be unconstitutional or otherwise illegal is deprived of a "fair" proceeding as well as "adequate … facilities" for the preparation of his or her defense. In particular, she or he is deprived of the opportunity to argue that evidence obtained through or derived from unlawful investigative methods should be excluded from the trial as "fruit of the poisonous tree"—a crucial remedy in the United States system for violations of constitutionally protected rights, including privacy rights. Additionally, parallel construction may be preventing defendants from being notified that they have been surveilled (or that some other measure interfering with privacy has been involved in their cases).

In *Arizona v. Wakil*, for example, a "whisper stop" in Arizona was used to conceal the government's warrantless use of a location-tracking device it had installed on the defendant's rental car—a practice that the defense argued was unlawful and that the US Supreme Court later held to be unconstitutional nationwide. The judge in the state-court case in Arizona eventually overturned Wakil's conviction due to this illegal monitoring, rejecting the prosecution's argument that there had been an "independent basis" for the

---

[222] See *Malone v. United Kingdom*, application no. 8691/79, judgment (European Court of Human Rights, plenary), August 2, 1984, ¶ 67; see also Office of the United Nations High Commissioner for Human Rights, "The right to privacy in the digital age," U.N. Doc. A/HRC/27/37, (2014), ¶ 23 ("[A]ny limitation to privacy rights reflected in article 17 must be provided for by law, and the law must be sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances"), available at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (accessed December 20, 2017) (hereinafter "OHCHR Report").

[223] See, e.g., *Szabó and Vissy v. Hungary*, application no. 37138/14, judgment (European Court of Human Rights), January 12, 2016, ¶ 86; see also OHCHR Report, ¶ 40.

[224] ICCPR, art. 2(3).

subsequent traffic stop (an improper windshield attachment).[225] This development would not have occurred if it had not emerged during proceedings in federal court the stop had been pretextual.[226]

In another case, *United States v. Mohamud*, the defendant was only able to challenge the constitutionality of the surveillance of his communications under Section 702 of FISA (and argue that the resulting evidence should have been excluded) because the government eventually provided notice that the surveillance had occurred.[227] At the time of writing, Mohamud had asked the US Supreme Court to rule on the constitutionality of the monitoring but the court had not yet indicated whether it would hear the case.[228]

"We … lack notice of all the surveillance techniques that were used [in the government's investigation], and also how they were used," the defense attorneys in *United States v. Al-Jayab* told an Illinois federal court in March 2017. "Without notice, Defendant cannot test whether the government's evidence was, in fact, lawfully obtained—or whether government surveillance conducted with limited or no court review violated his rights."[229]

Parallel construction may also deprive a defendant of exculpatory information, as well as the opportunity to contend that the investigative source or method the government has employed produces evidence that is inaccurate, incomplete, biased, or otherwise flawed. To the extent that the technique also prevents judges from understanding and evaluating the government's methods, it may also deprive defendants of a hearing by a "competent" tribunal.

---

[225] *Arizona v. Wakil*, Case no. CR-2011-00530 (Coconino County), Minute Entry, Nov. 6, 2014. The US Supreme Court ruled in *United States v. Jones*, 132 S.Ct. 945 (2012), that the Fourth Amendment warrant requirement applies to the monitoring of a vehicle's movements through the attachment and use of a GPS device.

[226] See *United States v. Wakil*, case no. 2:12-cr-00527 (C.D. Cal.), Report of Investigation (DEA Form 6) (doc. 321), filed July 7, 2013.

[227] See *United States v. Mohamud*, case no. 3:10-cr-00475 (D. Or.), Memorandum in Support of Motion for Full Discovery Regarding the Facts and Circumstances Underlying Surveillance (doc. 489), January 13, 2014; *United States v. Mohamud*, case no. 14-30217 (9th Cir.), Opening Brief of Appellant, September. 4, 2015, p. 137.

[228] Maxine Bernstein, "Mohamed Mohamud's lawyers petition U.S. Supreme Court to review conviction," *Oregonian/OregonLive*, July 14, 2017, http://www.oregonlive.com/portland/index.ssf/2017/07/mohamed_mohamuds_lawyers_petit.html (accessed October 19, 2017).

[229] *United States v. Al-Jayab*, case no. 1:16-cr-00181, Defendant's Motion for Notice of Surveillance Techniques Used During the Course of the Investigation (doc. 52), March 14, 2017, pp. 7-8.

Where the specific parallel construction technique of pretextual traffic stops is concerned, the demand for law enforcement officers to find an independent reason to stop and search a particular person or vehicle raises a risk that those officers will engage in unlawful behaviors in order to carry out this secretive task. Those behaviors may include the illegal prolongation of a stop,[230] unjustified "frisks"[231] and canine sniffs,[232] questioning that circumvents defendants' rights against self-incrimination,[233] and—as Judge Berzon wrote in her 2016 concurring opinion—"flat out lies about what police officers saw,"[234] which may constitute perjury if repeated in court.

At a broader level, parallel construction also creates a risk that the outcome of a case, and thus the consistency of the justice system for both defendants and any victims, will depend on how willing a defense attorney is to press for the revelation of undisclosed methods—particularly those that would be classified. 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.[235] One of the DEA trainings Ciaramella obtained also refers to the dismissal of a case as "the last resort" to protect the information a traffic stop was intended to "wall[] off." (The training adds: "Bottom line: DEA will rarely if ever disclose privileged or sensitive information from the other side of the 'wall.'"[236]) Therefore, 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. This situation jeopardizes the fairness and equality of trial processes.

---

[230] See, e.g., *United States v. Evans*.

[231] See, e.g., *United States v. Noble*.

[232] See, e.g., *United States v. Evans*.

[233] See, e.g., *United States v. Hernandez-Rodriguez*, 2012 U.S. Dist. LEXIS 31918 (M.D. NC), March 7, 2012, although no violation was found in this case.

[234] *United States v. Magallon-Lopez*.

[235] Human Rights Watch telephone interview with Robert Litt, former General Counsel of the Office of the Director of National Intelligence, August 29, 2017; Human Rights Watch interview with Arthur Rizer, Washington, DC, June 8, 2017.

[236] Muckrock documents, p. 203 of the complete PDF. Another training, which is undated, suggests that the government has only dismissed a case for this reason on one occasion, although the training appears to be referring to scenarios in which a judge has reviewed classified evidence by holding CIPA proceedings and determined that the evidence should be disclosed. Ibid. at pp. 60-61.

The shield of secrecy parallel construction creates also means that the public and even Congress may not realize that the executive branch is interpreting surveillance laws as allowing certain activities—violating the human rights requirement that such laws be clear and have foreseeable consequences. Furthermore, the public is unlikely to pressure Congress to change the laws or impose greater transparency requirements—crucial means of reining in executive power in democratic societies—if it is unaware of the surveillance taking place.

Defense attorneys interviewed by Human Rights Watch were scathing in their assessments of parallel construction.

"It is lying," said Azar-Farr, the Texas-based defense attorney who represented Syed Ali. "You [government agents] are lying to your higher-ups, you are lying to your prosecutors, you are lying to the judge in the case, you are lying to the defense lawyer, you are lying to the accused."[237] The government, he said, "know[s] [parallel construction] is illegal and you're not supposed to do this. And they still do it. Maybe because they find it necessary, maybe they're guided by a desire to ensure that bad people get arrested and are put in prison."[238] He could understand these motivations, he said. "But you're not doing the United States any good when you behave like this."[239]

Similarly, Missouri defense attorney Dan Viets described parallel construction as "lying. Just lying." "All they [the government] are doing is just lying. And they're lying to the courts. I guess I'm naïve about this, but I would think that judges would be offended that this is [the government's] standard operating procedure." He went on, "In some cases, the prosecutors are victims; in some cases, they are collaborators with these lies that are being told to the courts. It's just appalling." He continued, "Surely, due process requires that the police don't lie to the courts, that prosecutors don't lie to the court."[240]

[237] Human Rights Watch telephone interview with attorney Simon Azar-Farr, San Antonio, Texas, June 1, 2017.
[238] Ibid.
[239] Ibid.
[240] Human Rights Watch telephone interview with defense attorney Dan Viets, Columbia, Missouri, April 3, 2017.

Michigan attorney John Minock commented that parallel construction troubles him "because it's a fiction. It's a lie. It's a means of disguising illegal intercepts and warrantless searches."[241]

Carmichael, one of the defense attorneys in *Collins*, told Human Rights Watch that parallel construction "flies in the face of everything that our justice system stands for" and is "legally and as a matter of principle a huge problem. We have in our country a Fourth Amendment and Fourth Amendment rights … That's a bedrock principle of our system. Essentially, this practice is an attempt to circumvent that. It's a way that defendants can't challenge the evidence and the way that it was obtained."[242]

Brian Pori, a federal public defender in New Mexico, said of parallel construction: "One practical effect is that it encourages law enforcement to be duplicitous. Law enforcement should not have to pretend—they shouldn't have to keep one hand behind their back with the information that they have." He added, "Any honorable law enforcement officer or prosecutor can figure out an honorable way to do the things that they're doing. Why do we have to have this charade or this game?"[243]

Several of these defense attorneys took pains to stress that they understood the value of intelligence-gathering.[244] However, Kiyonaga—one of the other defense attorneys in *Collins*—noted when interviewed, "National security shouldn't be allowed to eviscerate the Fourth Amendment and the other procedural safeguards that attend a prosecution."[245] Similarly, Azar-Farr accepted the idea of congressionally-approved intelligence collection to "prevent threats to the sovereignty of the nation."[246] "But don't collect all of this information," he said, "and then tell me that you have used it to arrest the guy who happened to sell half a kilo of marijuana in the suburbs of Philadelphia."[247]

---

[241] Human Rights Watch telephone interview with defense attorney John Minock, Ann Arbor, Michigan, May 12, 2016.

[242] Human Rights Watch telephone interview with defense attorney Jessica Carmichael, Alexandria, Virginia, July 24, 2017.

[243] Human Rights Watch telephone interview with Brian Pori, Assistant Federal Public Defender, Albuquerque, New Mexico, March 15, 2017.

[244] Ibid.; Human Rights Watch telephone interview with attorney Simon Azar-Farr, San Antonio, Texas, June 1, 2017; Human Rights Watch telephone interview with defense attorney Jessica Carmichael, Alexandria, Virginia, July 24, 2017.

[245] Human Rights Watch interview with defense attorneys John Kiyonaga and Marina Medvin, Alexandria, Virginia, May 12, 2016.

[246] Human Rights Watch telephone interview with attorney Simon Azar-Farr, San Antonio, Texas, June 1, 2017.

[247] Ibid.

"Think of it a little differently," Azar-Farr said. "[I]f the doors were open that you could use any information [from] counterintelligence information as part of [prosecutions] in criminal courts, then you might as well say that we don't have a Fourth Amendment. Taken to its logical extension, there would be no Fourth Amendment."[248]

Alvaro Bedoya, an attorney and the executive director of the Center on Privacy & Technology at Georgetown Law, described parallel construction to Human Rights Watch as "antithetical to the core of due process" and pointed out that it may prevent judges from evaluating the legality of new types of surveillance technologies such as facial recognition software.[249] The defense attorneys in *Al-Jayab* made the same point, writing that "notice and discovery are especially crucial in an era of rapidly changing technology. By withholding notice, the government is preventing defendants from challenging sweeping new forms of surveillance that have never been reviewed in any adversarial court proceeding."[250] The research described in this report supports the gravity of these concerns.

[248] Ibid.

[249] Human Rights Watch telephone interview with Alvaro Bedoya, Executive Director, Center on Privacy & Technology, Georgetown Law, Washington, DC, June 30, 2017.

[250] *United States v. Al-Jayab*, doc. 52, p. 18.

V. Recommendations

To eliminate the human rights violations that parallel construction entails, Human Rights Watch recommends that Congress address the issue directly through legislation. Specifically, we recommend that the body adopt laws to require the disclosure to criminal defendants of complete information about the origins of the investigations in their cases, with special procedures as necessary to address classified information or information whose disclosure may jeopardize the lives or safety of identifiable human informants. Such procedures should be conducted by judges and should ensure that defense counsel have sufficient access to the information to challenge potentially unlawful activity. They should prohibit the sanitization of information in a manner that precludes constitutional or other challenges to the legality of a government activity that led to the identification of information or evidence.

Congress should also adopt legislation requiring that all executive branch agencies be treated as part of the prosecution for the purposes of obligations to disclose exculpatory information. Additionally, it should evaluate the judicially developed doctrines (such as applications of the "independent source" doctrine, interpretations of *Whren*, and the doctrine of collective knowledge) that may facilitate law enforcement's use of searches and seizures for parallel construction purposes and consider imposing restrictions accordingly.

To address the possibility that parallel construction is used to conceal potentially unconstitutional surveillance, we recommend that Congress adopt legislation strictly requiring the executive branch to notify defendants in all criminal cases of any employment of investigative techniques involving the surveillance of communications or metadata, or the compilation or monitoring of other personal data such as biometric data. Congress should also adopt similar requirements for other proceedings in which individuals' rights are adjudicated (such as immigration proceedings). Such legislation should impose requirements on prosecutors to determine whether such techniques were employed. In general, Congress should exercise stronger oversight over surveillance and other forms of data-gathering that take place under intelligence authorities.

The US executive branch should also act to eliminate parallel construction. Human Rights Watch recommends that the Justice Department adopt policies prohibiting the practice and

publicly disclose all relevant policies and legal interpretations. The Justice Department should also provide clear and publicly available legal guidance to the FBI, the DEA, and other relevant entities regarding these matters. Human Rights Watch also regards measures by ODNI as necessary: the Director of National Intelligence should publicly and fully disclose all policies and legal interpretations that may affect criminal defendants or others involved in proceedings before US courts or tribunals, including where these policies or interpretations conclude that an activity or approach will not result in any violations of rights.

The US federal and state courts will also be critical in ending the rights violations that parallel construction entails or may promote. When the circumstances of a case suggest that the government may have engaged in parallel construction to conceal activities that could have implications for the defendant's rights, Human Rights Watch recommends that judges strongly consider directing the prosecution to disclose any previously unrevealed investigative sources or techniques that were employed in the case or otherwise led to evidence, including by directing it to make inquiries with relevant law enforcement and intelligence bodies. They should consider issuing such orders even in the absence of specific evidence of parallel construction or the activities it may have been used to conceal, since the practice is designed to prevent defendants from possessing such evidence.

Human Rights Watch further recommends that when courts consider cases that may involve parallel construction, they should apply any relevant common-law doctrines, including those pertaining to pretextual traffic stops, the collective-knowledge doctrine, and the independent-source doctrine, in a manner that fully comports with human rights and the US Constitution. The US Supreme Court should consider revisiting or clarifying previous decisions that are currently facilitating parallel construction (or the problematic practices the executive branch may be employing it to conceal).

Conclusion

Fair-trial rights and the rights of people under investigation are so deeply woven into the US Constitution and human rights laws as to be inextricable from them. Both the Constitution and human rights treaties demand fair play and respect for the value of an individual's liberty. In the US, the Constitution's Fourth, Fifth, and Fourteenth Amendments are vital in creating and ensuring a legal system that is truly just.

Parallel construction fails that test. At best, it displaces judges from their role of deciding which government behaviors respect rights and which do not. At worst, it is a legalistic form of deceit, one that renders proceedings unfair and may ensure that violations of rights—not only of defendants, but of the US population at large—stay in the shadows, undetected and unchallenged. Its existence poses a threat to the bedrock concepts of a presumption of innocence and the gravity of the loss of liberty through imprisonment. This report shows that parallel construction is real, may be occurring regularly, and in a democratic society, should be disallowed.

Acknowledgments

This report was compiled and written by Sarah St.Vincent, researcher and advocate on US national security, surveillance, and domestic law enforcement. Significant research, proofreading, and formatting assistance was provided by W. Paul Smith, Maya Goldman, and Thomas Rachko, associates in the US Program at Human Rights Watch. The report was reviewed and edited by John Raphling, senior US criminal justice researcher; Cynthia Wong, senior researcher on the internet and human rights; Alison Parker, US Program director; Dinah PoKempner, general counsel; and Joe Saunders, deputy program director. Much of the research was supervised by Maria McFarland Sánchez-Moreno, co-director of the US Program until August 2017. Layout and production were managed by Rebecca Rom-Frank, publications coordinator, and Fitzroy Hepkins, mail manager for Human Rights Watch.

Human Rights Watch wishes to thank Patrick Toomey, staff attorney in the American Civil Liberties Union's National Security Project, for sharing potential parallel construction cases and providing invaluable comments on a draft of this report. We also greatly appreciate helpful comments on the draft offered by David Kris, an adviser at Intellectual Ventures and a former assistant attorney general for national security. Jumana Musa, senior privacy and national security counsel at the National Association of Criminal Defense Lawyers, and Lee Tucker, assistant federal defender in the Tucson, Arizona Office of the Federal Defender, provided us with crucial assistance in disseminating our request for information about potential instances of parallel construction to US defense attorneys. This report does not necessarily reflect the views of these individuals or their employers, and their participation does not constitute endorsement.

Above all, we wish to thank the defense attorneys who generously took the time to speak with us—sometimes repeatedly—and provide us with case records, as well as the current and former US government officials who shared their views with thoughtfulness and candor.

Annex: Background on US Surveillance Authorities

A. The Fourth, Fifth, and Fourteenth Amendments to the US Constitution

In the mid-18th century, fierce controversies arose in what is now the United States over the British colonial authorities' sweeping and intrusive methods for finding evidence of customs violations or materials criticizing the government.[251] Largely in response to these excesses, the US Constitution contains the Fourth Amendment, which reads:

> 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.[252]

Questions about how to apply these Fourth Amendment protections to evolving technologies have given rise to a complex body of US Supreme Court case law that has shaped US surveillance practices as well as some of parallel construction's many forms.

B. Law Enforcement Surveillance and Other Search Powers

1. *Access to telephone and internet communications: content*

Nearly 90 years ago, the US Supreme Court began grappling with how to apply the Fourth Amendment—which, as noted above, broadly requires the government to obtain a warrant before conducting searches or seizures—to a new type of communications device: the telephone.[253] Eventually, the court held that the Fourth Amendment's protections apply to the recording of conversations—including phone calls.[254]

---

[251] *See Boyd v. United States*, 116 U.S. 616, 623-630 (1886); *United States v. Verdugo-Urquidez*; Clark D. Cunningham, "Apple and the American Revolution: Remembering Why We Have the Fourth Amendment," Forum post, *Yale Law Journal*, October 26, 2016, https://www.yalelawjournal.org/forum/apple-and-the-american-revolution-remembering-why-we-have-the-fourth-amendment-1 (accessed November 6, 2017).

[252] US Constitution, Fourth Amendment.

[253] *Olmstead v. United States*, 277 U.S. 438 (1928).

[254] *Katz v. United States*, 389 U.S. 347 (1967).

Congress went on to enshrine this ruling in statutory law when it adopted the Omnibus Crime Control and Safe Streets Act of 1968. Title III of the law, which is sometimes known as the Wiretap Act and which Congress has since amended several times, generally prohibits individuals from intercepting "any wire, oral, or electronic communication."[255] The law makes an exception for authorities who have obtained a warrant from a judge based on probable cause to believe that someone has committed or will soon commit a certain type of crime. The authorities must also show, among other things, that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous."[256] In 1986, Congress extended the scope of the original Wiretap Act to include electronic communications by adopting the Electronic Communications Privacy Act.[257]

While the Wiretap Act (as amended) is foundational to US communications privacy, in 2016 journalists uncovered a "vast and legally questionable eavesdropping program" created by the DEA and federal prosecutors and involving the interception of "millions of calls and text messages based on the approval of a single state-court judge" in California.[258] This development raises concerns as to whether the government's approach to surveillance even under Title III (a relatively uncontroversial law) has been fully disclosed or itself raises constitutional concerns.

---

[255] 18 U.S.C. § 2511.

[256] 18 U.S.C. §§ 2516, 2518.

[257] See Justice Information Sharing, "Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510-22," Department of Justice, July 30, 2013, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285; Electronic Privacy Information Center, "Electronic Communications Privacy Act (ECPA)," https://epic.org/privacy/ecpa/. While ECPA's provisions are complex, they generally establish that law enforcement must obtain a warrant to intercept the content of e-mails, chats, direct messages on social media sites, and other electronic communications while those communications are being transmitted. Law enforcement's powers to gain access to the content of stored electronic communications depend on where those communications are stored (for example, on an internet company's server or a personal device), how old they are, and whether the recipient has opened them. Civil-society groups have long sought reforms to ECPA to improve the consistency of its rights protections.

[258] Brad Heath, "DEA changes wiretap procedure after questionable eavesdropping case," *USA Today*, July 7, 2016, https://www.usatoday.com/story/news/2016/07/07/dea-changes-wiretap-procedure-after-questionable-eavesdropping-cases/86802508/ (accessed November 6, 2017). In at least one case, prosecutors later determined that these wiretaps had been illegal: see Brad Heath and Brett Kelman, "After illegal wiretap, suspects go free and want a refund," *USA Today*, December 9, 2015, https://www.desertsun.com/story/news/2015/12/09/illegal-dea-wiretap-riverside-money-laundering/77050442/ (accessed November 1, 2017).

2. Access to telephone and internet communications: metadata

US law draws distinctions between the content of communications and information that describes those communications without directly revealing what they contain—for example, the date and duration of a telephone call, as well as the numbers of the caller and recipient. Surveillance experts often refer to this type of descriptive information as "metadata" (although the term itself does not have a legal meaning or an agreed technical one).

In 1979, the US Supreme Court held in *Smith v. Maryland* that individuals do not have a reasonable expectation of privacy in the telephone numbers they dial—meaning that the Fourth Amendment does not require law enforcement officers to obtain a warrant before seeking such information.[259] This ruling continues to underpin US legal theories premised on the idea that metadata does not require the same protections as the content of communications.[260]

3. The surveillance of non-US Persons outside the United States

In a 1990 case about the DEA's warrantless search of a Mexican citizen's physical property in Mexico, the US Supreme Court stated that the Constitution's drafters did not intend for the Fourth Amendment "to apply to activities of the United States directed against aliens in foreign territory or in international waters."[261] This reasoning now forms a significant part of the legal underpinning for the country's warrantless intelligence surveillance programs, which, when targeted in nature, purport only to target "non-United States persons." ("United States persons" is a legal category that includes US citizens, lawful permanent residents—commonly known as green-card holders—and some corporations and associations.[262])

C. Intelligence and National Security Surveillance Powers

The use of surveillance in the United States for intelligence purposes has historically been far more controversial than monitoring in the law enforcement context, and the interplay between the intelligence bodies and the criminal justice system has long been fraught with

---

[259] *Smith v. Maryland*.

[260] See *United States v. Jones* (Sotomayor, J., concurring).

[261] *United States v. Verdugo-Urquidez*.

[262] 50 U.S.C. § 1801(i).

concerns about potential abuses.[263] In criticizing the excessive and discriminatory intelligence surveillance activities of the mid-20th century, an influential Senate panel commonly known as the Church Committee distinguished intelligence activity from criminal investigations. Its members wrote in 1976:

> It is, of course, proper in many circumstances—such as developing a criminal prosecution—for the Government to gather information about a citizen and use it to achieve legitimate ends, some of which might be detrimental to the citizen. But in criminal prosecutions, the courts have struck a balance between protecting the rights of the accused citizen and protecting the society which suffers the consequences of crime. Essential to the balancing process are the rules of criminal law which circumscribe the techniques for gathering evidence, the kinds of evidence that may be collected, and the uses to which that evidence may be put. In addition, the criminal defendant is given an opportunity to discover and then challenge the legality of how the Government collected information about him and the use which the Government intends to make of that information.[264]

As demonstrated in this report, today parallel construction risks seriously undermining the "opportunity to discover and then challenge the legality of how the Government collected" and uses information. This, in turn, raises the risk that the government—operating without sufficient accountability or oversight—will engage in abuses.

In the wake of revelations about the mid-20th-century excesses addressed in the Church Committee's report, Congress and the executive branch began to impose stronger restrictions on the intelligence agencies, including where surveillance is concerned.[265] However, over time, and particularly following the attacks of September 11, 2001, these protections have eroded.

---

[263] See, e.g., David S. Kris and J. Douglas Wilson, *National Security Investigations & Prosecutions 2d* (Thomson West, 2012), vol. II, pp. 5-13.

[264] Ibid., vol. I, pp. 38-44; Church Committee Report, Book II, pp. 2-3 (internal citation omitted).

[265] See, e.g., Kris and Wilson, vol. I, pp. 49-62; Foreign Intelligence Surveillance Act of 1978.

1. The Foreign Intelligence Surveillance Act

a. FISA orders

In 1978, Congress made it clear that even when the executive branch had a foreign intelligence purpose for conducting surveillance from within the US, it needed to get a judicial warrant in each case. The Foreign Intelligence Surveillance Act ("FISA") required—and, for surveillance that is carried out in the United States and targets a US person, still requires—that government agents obtain an individualized order based on a sworn statement showing probable cause to believe that the target is a "foreign power" (or "agent of a foreign power") and certifying that the information sought "cannot reasonably be obtained by normal investigative techniques."[266]

b. Section 702 of FISA

In 2005, the *New York Times* revealed that the executive branch had been monitoring the international telephone and internet communications of people in the United States, based on an executive order and without obtaining warrants.[267] After much controversy, Congress responded by ultimately adopting the FISA Amendments Act ("FAA") in 2008. The FAA added a set of provisions to FISA, including Section 702.[268]

Section 702 empowers the intelligence agencies to "target" non-US persons overseas for warrantless telephone or internet monitoring.[269] The purposes for which the government may conduct such monitoring are expansive: the executive branch need only certify that "a significant purpose" of the surveillance is to obtain "foreign intelligence information."[270] FISA defines this term broadly to include, for example, "information with respect to a foreign power or foreign territory that relates to … the conduct of the foreign affairs of the United States."[271] Hypothetically, information about a foreign march for civil rights or

---

[266] See 50 U.S.C. § 1804(a). This requirement also applies to electronic surveillance carried out in the United States that targets *non*-US persons, although the FISA Amendments Act (explained below) also allows the government to carry out warrantless surveillance targeting such persons if they are outside the United States.

[267] James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, December 16, 2005, http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html (accessed November 6, 2017).

[268] FISA Amendments Act of 2008, available at https://www.gpo.gov/fdsys/pkg/BILLS-110hr6304enr/pdf/BILLS-110hr6304enr.pdf (accessed November 6, 2017).

[269] 50 U.S.C. §1881a(a)-(b).

[270] 50 U.S.C. § 1881a(g)(2)(A)(v).

[271] 50 U.S.C. § 1801(e).

relating to a foreign agency's decision to restrict the sale of a particular substance such as tobacco, for example, would appear to qualify. The government reported having an estimated 106,469 targets under Section 702 in 2016 (the most recent year for which data is available).[272]

Although US persons cannot be the official targets of Section 702 surveillance and the statute prohibits reverse targeting—that is, the deliberate targeting of a non-US person with the actual goal of surveilling a US person—the government believes it has the power to surveil US persons' communications "incidentally." For example, if a US person Skypes with an uncle in China, calls a business in Mexico, e-mails a professor in Germany, or sends a Facebook message to a friend in India, the US government believes it is entitled to sweep up those communications without a warrant if any of those people or entities are the non-US person targets of Section 702 surveillance. At the time of writing, the scale of the government's "incidental" capture of US persons' information under Section 702 was unknown, although a 2014 report by the independent Privacy and Civil Liberties Oversight Board ("PCLOB") characterized it as "potentially large" and another independent expert described it in 2015 as "broad."[273]

The PCLOB's 2014 report confirmed that the government has operated at least two massive warrantless surveillance programs pursuant to this provision.[274] One, "upstream" scanning, has allegedly involved the automated bulk searching of communications that flow over the internet infrastructure that links the US to the rest of the globe.[275] The other, PRISM, has enabled the NSA—with the FBI's assistance—to demand private communications such as e-mails and instant messages from US internet companies without warrants.[276] Documents disclosed by former NSA contractor Edward Snowden

---

[272] Office of the Director of National Intelligence, "Statistical Transparency Report Regarding the Use of National Security Authorities for Calendar Year 2016," April 2017, p. 7, https://www.dni.gov/files/icotr/ic_transparecy_report_cy2016_5_2_17.pdf (accessed November 6, 2017).

[273] PCLOB Report, p. 9; Brief of *Amicus Curiae*, United States Foreign Intelligence Surveillance Court, Oct. 16, 2015, p. 11, available at https://www.aclu.org/foia-document/brief-fisc-amicus-curiae-amy-jeffress?redirect=foia-document/brief-amicus-curiae (accessed November 6, 2017).

[274] PCLOB Report.

[275] See Ashley Gorski and Patrick Toomey, "Unprecedented and Unlawful: The NSA's 'Upstream' Surveillance," post to American Civil Liberties Union (blog), September 23, 2016, https://www.aclu.org/blog/speak-freely/unprecedented-and-unlawful-nsas-upstream-surveillance (accessed November 6, 2017).

[276] PCLOB Report, pp. 33-34.

beginning in 2013 indicate that these companies have included Google, Apple, Microsoft, and Facebook, among others.[277]

Section 702 requires the government to submit annual "targeting" and "minimization" procedures to the Foreign Intelligence Surveillance Court—procedures that are supposed to provide some privacy protections to US persons.[278] ("Minimization" refers to the practice of preventing the gathering or sharing of information that concerns or identifies US persons.[279]) However, the court does not issue individualized warrants or review the government's individual targeting decisions.

As explained below, the NSA may share specific information gathered under Section 702 with the FBI in a broad set of circumstances. The FBI may also search (or "query") raw Section 702 data—that is, the data as it was originally obtained—without a warrant, including by using search terms related to US persons, to find "foreign intelligence information" or "evidence of a crime."[280]

At the time of writing, Section 702 was scheduled to expire on December 31, 2017, unless Congress renewed it.[281]

2. Intelligence-sharing arrangements with foreign governments

EO 12333 allows the Director of National Intelligence to "enter into intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations."[282] These agreements do not require the approval of Congress.

---

[277] See "NSA slides explain the PRISM data-collection program," *Washington Post*, July 10, 2013, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (accessed November 6, 2017).

[278] 50 U.S.C. § 1881a(d)-(e).

[279] See 50 U.S.C. § 1801(h).

[280] "Minimization Procedures Used by the Federal Bureau of Investigation in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, As Amended," September 21, 2016, p. 11, https://www.dni.gov/files/documents/icotr/51117/2016_FBI_Section_702_Minimization_Procedures_Sep_26_2016_part_1_and_part_2_merged.pdf (accessed November 6, 2017) (hereinafter "FBI minimization procedures").

[281] FISA Amendments Act Renewal Act of 2012, available at https://www.intelligence.senate.gov/sites/default/files/legislation/hr5949.pdf (accessed November 6, 2017).

[282] Executive Order 12333, "United States Intelligence Activities" (as amended 2008), § 1.4(b)(4)(A).

The executive branch has released certain historical documents concerning an intelligence-sharing agreement between the US and the United Kingdom,[283] and Snowden disclosed a memorandum of understanding suggesting that the US shares raw surveillance data with Israel.[284] However, Human Rights Watch is unaware of any intelligence-sharing arrangements whose current scope or details the government has made available to the public.

In a 2014 interview with Human Rights Watch, a senior US intelligence official stated that the government is permitted to *receive* intelligence concerning US persons from foreign states even in circumstances in which it would be illegal for the US to conduct the surveillance itself, although the authorities cannot *request* such intelligence.[285]

More recently, as part of the Senate Select Committee on Intelligence's confirmation hearing for CIA Director Mike Pompeo in 2017, Senator Ron Wyden stated:

> Absent a specific request from the CIA, a foreign partner, company, organization or individual may nonetheless provide the CIA with the results of extensive cyber operations or other surveillance, including targeted collection against, or bulk collection that includes the communications of U.S. persons. That information could include the communications of U.S. political figures and political activists, leaders of nonprofit organizations, journalists, religious leaders, businesspeople whose interests conflict with those of President Trump, and countless innocent Americans.[286]

3. The sharing of intelligence with law enforcement

After the attacks of September 11, 2001, questions about the extent to which the intelligence agencies may and should share information with law enforcement bodies

---

[283] National Security Agency/Central Security Service, "UKUSA Agreement Release: 1940-1956," May 3, 2016, https://www.nsa.gov/news-features/declassified-documents/ukusa/ (accessed November 6, 2017).

[284] "Memorandum of Understanding (MOU) Between the National Security Agency/Central Security Service (NSA/CSS) and the Israeli SIGINT National Unit (ISNU) Pertaining to the Protection of U.S. Persons," undated, available at http://www.statewatch.org/news/2013/sep/nsa-israel-spy-share.pdf (accessed November 6, 2017).

[285] Human Rights Watch, *With Liberty to Monitor All* (New York: Human Rights Watch, 2014), https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and.

[286] "Questions for the Record: Mike Pompeo" (completed), Senate Select Committee on Intelligence, January 18, 2017, p. 5, https://www.intelligence.senate.gov/sites/default/files/documents/qfr-011217.pdf (accessed November 6, 2017).

gained new urgency. In US public discourse, the attacks were widely portrayed as having resulted from a failure on the part of intelligence and law enforcement agencies to "connect the dots"—that is, to obtain and share relevant information with one another.[287] Public commentary that emerged after the attacks also decried a phenomenon known as "The Wall": bureaucratic restrictions that gradually came to impede the sharing of intelligence information with prosecutors assigned to non-terrorism criminal cases, and that the 9/11 Commission ultimately described as "misunderstood and misapplied."[288]

Today, the government has adopted procedures that allow Section 702 and EO 12333 surveillance data to be shared with law enforcement under a wide range of circumstances. For example, if the NSA "incidentally" captures communications to or from US persons as part of its warrantless surveillance under Section 702, it can share those communications with federal law enforcement if the messages contain "evidence of a crime that has been, is being, or is about to be committed."[289] Similarly, the FBI may disseminate information obtained under Section 702 concerning a US person that "reasonably appears to be evidence of a crime" to federal, state, local, and tribal law enforcement.[290] The sharing of this warrantlessly gathered data is itself warrantless and does not require any specific level of suspicion that the person concerned is engaged in criminal wrongdoing, giving rise to a risk that such sharing will effectively constitute an end-run around Fourth Amendment protections.

Less information is available about the sharing of information gathered under EO 12333. However, the NSA has publicly released procedures indicating that it may disseminate information about US persons that it has obtained under EO 12333 in a range of circumstances, including when "[t]he information is evidence of a possible commission of

---

[287] See National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (2004), p. 400, available at https://www.9-11commission.gov/report/911Report.pdf (accessed December 21, 2017).

[288] Ibid., p. 79; on public claims regarding "The Wall" and its role in the government's failure to prevent the attacks, see, e.g., Josh Meyer, "Fingers Point at an Intelligence 'Wall'," *L.A. Times*, April 14, 2004, http://articles.latimes.com/2004/apr/14/nation/na-wall14_ (accessed November 6, 2017).

[289] "Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, as Amended," March 24, 2017, pp. 10, 13 https://www.dni.gov/files/documents/icotr/51117/2016-NSA-702-Minimization-Procedures_Mar_30_17.pdf (accessed November 6, 2017).

[290] FBI minimization procedures, pp. 31-32.

a crime" or "indicates that the U.S. person may be engaged in international narcotics trafficking activities."[291]

4. Notification of surveillance

US law contains both statutory and (in some circumstances) constitutional requirements for the disclosure of surveillance to defendants. For example, the Wiretap Act requires that individuals named in a wiretap order must be notified of the surveillance after it has concluded.[292] The government must also notify a defendant (or other party, as applicable) if it plans to use wiretapped communications "or evidence derived therefrom" in proceedings.[293]

FISA, too, obligates the government to notify defendants or other parties in advance if it "intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding … against an aggrieved person, any information obtained or derived from an electronic surveillance [*sic*] of that aggrieved person."[294] However, civil society experts and defense attorneys have expressed concerns about the government's failure to disclose how it interprets this obligation—particularly the phrase "derived from"—in the Section 702 context.[295]

The government reportedly believes it is not required to notify any individual—including a criminal defendant—of the surveillance of his or her communications under EO 12333.[296]

---

[291] "Procedures for the Availability or Dissemination of Raw Signals Intelligence Information by the National Security Agency under Section 2.3 of Executive Order 12333 (Raw SIGINT Availability Procedures)", p. 12, January 3, 2017, https://fas.org/sgp/othergov/intel/sigint-raw.pdf (accessed November 6, 2017).

[292] 18 U.S.C. § 2518(8)(d).

[293] 18 U.S.C. § 2518(9).

[294] 50 U.S.C. § 1806(c). According to the law, an "aggrieved person" is someone who "is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." 50 U.S.C. § 1801(k).

[295] See, e.g., Toomey, "Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance – Again?"

[296] Savage, "Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide."