Parallel Construction

RESTORE the FOURTH

In a recent House Judiciary Committee hearing, "Oversight of the Federal Bureau of Investigation," Rep. Tom McClintock asked FBI Director Christopher Wray a simple question: "Can you describe the term parallel construction as it relates to evidence produced in FISA searches?" Wray avoided the question altogether:

"Parallel construction? I'm not sure I've used the term before...I'm just not sure about the use of the term."

McClintock pried further and asked, "Has the FBI ever employed that particular tactic in prosecuting American citizens?" Wray lied in reply, saying, "Not to my knowledge."

The remainder of this brief will explain what parallel construction is, and why this is a lie.[1]

What is Parallel Construction?

Parallel construction, also referred to as "alternative construction," occurs when law enforcement officials use an illegal method or technology, which they intend to hide, to search for criminal activity.[2] They cover their tracks by later using a legal way to access the same or similar evidence. The act of concealing illegal surveillance methods by instead using subsequent legally acquired evidence to launch an investigation is called parallel construction or "evidence laundering" because, like money laundering, it involves converting illegal evidence into legal evidence.[3]

How is evidence "converted" from illegal to legal?

United States v. Alverez-Tejeda (2007) is an egregious example of how parallel construction is deployed by law enforcement officials.[4] Ascension Alverez-Tejeda and his girlfriend were hit by a truck driver from behind. As Alverez-Tejeda walked out of his vehicle to inspect the damage, two police officers arrived at the scene and arrested the truck driver for a DUI. Law enforcement officers instructed Alverez-Tejeda and his girlfriend to sit in a police cruiser to await processing. Suddenly, someone jumped into Alverez-Tejeda's vehicle and drove off, launching a failed police chase in which, as far as Alverez-Tejeda knew, the car was not recovered.

The whole incident including the "drunk" truck driver and the car thief was a scheme orchestrated by DEA officials and law enforcement officers.[5] It was planned to obfuscate how the DEA originally learned of Alverez-Tejeda's alleged drug trafficking, mainly via illegally intercepted phone calls. Once the police obtained the car, they secured a search warrant and found cocaine and methamphetamine. A federal judge ruled that the DEA's complicated ploy violated Alverez-Tejeda's Fourth Amendment right to be free of warrantless and unreasonable searches and seizures.[6] However, an appeals court later overturned this ruling.[7]

Other parallel construction cases occur in the context of prosecutions for material support of terrorism. Fazliddin Kurbanov, an immigrant from Uzbekistan, was sentenced to 25 years in federal prison in 2016.[8] A few years after arriving in the U.S., Kurbanov was placed under FBI surveillance. During his trial, he was informed that spying on his communications with associates from the Islamic Movement of Uzbekistan was authorized under the Foreign Intelligence Surveillance Act of 1978. This was a lie.[9] Justice Department attorneys had instead illegally intercepted Kurbanov's communications under PRISM, an NSA mass surveillance program uncovered by documents leaked by Edward Snowden in 2013.[10] PRISM was a highly classified program that the NSA and FBI operated to retrieve Americans' private data directly from companies like Yahoo, Google, Facebook, and Apple. The same practices, now renamed "downstream surveillance", continue today.

Both Alverez-Tejeda and Kurbanov's cases emphasize key aspects of parallel construction. First, both investigations were launched based on information secured under legally questionable surveillance programs. Then, law enforcement worked closely with intelligence officials to conceal the origins of these investigations. In Alverez-Tejeda's case, by orchestrating a traffic incident to establish a basis for searching his vehicle. Often, there is no need for elaborate theatrics. Law enforcement officers frequently use pretextual traffic stops to knowingly preempt an investigation based on intelligence information.[11] Unfortunately, in *Whren v. U. S.* (1996) the Supreme Court has blessed this practice.[12] Intelligence gathering tools meant for national security

purposes were deployed in domestic criminal contexts in the cases of Alvarez-Tejeda and Kurbanov. Due process requires that suspects be permitted to discover and challenge the manner by which the evidence against them was gathered, rather than permanently insulating intelligence collection methods from court review. The inevitable result of that insulation is that parallel construction becomes the rule, and illegal searches cannot be challenged.

The nature of parallel construction, and its recent emergence into public knowledge, makes it difficult to know for certain the true scope of its practice.[13] However, we do know that multiple federal agencies are guilty of it.

DEA's Hemisphere Program and the "Dark Side"

The Drug Enforcement Agency (DEA) is the nexus of NSA data distribution.[14] A subdivision of the DEA, known as the Special Operations Division (SOD), is tasked with distributing information to law enforcement agents for the purpose of launching investigations.[15] A typical example is that after surveilling communications of millions of individuals, someone discussing a cross-border drug trade is identified. Law enforcement is informed and then follows the individual when they set out to cross the border. CBP is notified when the suspect reaches the border so they can legally search the vehicle and find the drugs because searches at the border do not require probable cause or even reasonable suspicion of a crime.[16]

The SOD, colloquially referred to by agents as the "Dark Side," is comprised of representatives from at least two dozen other agencies, including the FBI, NSA, CIA, IRS, and DHS.[17] Originally created to curtail Latin American drug cartels, the SOD has far exceeded its mandate. Its vast cross-intelligence agency work suggests that parallel construction is a widespread practice.

Like the NSA's mass collection of Americans' phone records, the DEA runs the Hemisphere Program (generally referred to simply as "Hemisphere") in partnership with AT&T.[18] Hemisphere captures four billion call records a day.[19] AT&T embeds employees with police agencies in hubs located in Houston, Atlanta, and Los Angeles. As the Electronic Frontier Foundation explains, "These employees run the software that searches and analyzes AT&T's massive phone database. Cops country wide who work drug cases, contact their regional hub to get the records which federal officials collected by querying Hemisphere without ever getting permission from a judge."[20] A 2019 report indicates that Hemisphere, which was first exposed in 2013 after operating for 6 years, still exists under the pseudonym, "Project C."[21]

"Project C" (Hemisphere) collects metadata which are records of phone call locations, times, participants, and lengths, devoid of any content. This mosaic of information is ripe for pattern analysis, enabling law enforcement officers to track personal lives and physical locations. Under the Supreme Court's ruling in *Carpenter v. United States*, historic cell site location information may only be accessed with a warrant based on probable cause. Parallel construction ensures that "Project C" does not see the light of day or the scrutiny of the court. It is likely that "Project C" data access has expanded well beyond the DEA. In 2017, it was reported that police departments pay from $100,000 to $1 million a year for Hemisphere access.[22]

Recent bombshell reporting indicates that "Project C" has been renamed Data Analytical Services (DAS).[23] Funding for Hemisphere was suspended by former U.S. president Barack Obama in 2013. Even though discretionary funding was frozen for three years, records obtained by WIRED indicate that individual law enforcement organizations were permitted to contract with AT&T to maintain access to its phone records. Funding was halted again in 2021 but resumed in 2022 under President Joe Biden, despite the Supreme Court's holding in *Carpenter v. United States* that Americans have a reasonable expectation of privacy in their location data.[24]

The scope of DAS is striking. It casts a wider dragnet than the telephone metadata program operated by the NSA, which was shuttered in 2014 after its collection was deemed illegal by the U.S. Second Circuit Court of Appeals.[25] The latter was the program that Edward Snowden leaked to the American public in 2013. DAS was first disclosed by the New

York Times in 2013 as Hemisphere. Since then, law enforcement agents have been instructed to never "refer to Hemisphere in any official document."[26]

DEA training documents were obtained via a Freedom of Information Act (FOIA) request filed by journalist CJ Ciaramella in 2013.[27] They reveal that parallel construction was not only encouraged but required for all agents. In the training module, agents were told that "Classified Material must be protected: To use it, we must protect, or lose it." It was explicitly stated that one of the course objectives was for agents to be capable of "[Articulating] 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."[28]

Law enforcement officials are trained to engage in parallel construction to skirt Fourth Amendment protections. In *U.S. v. Grobstein* (2013), a federal case in New Mexico, security videos from an Albuquerque bus station show a DEA agent secretly and unlawfully searching a bag that was left on a bus during a layover.[29] Once the passengers reboard, the officer asked for consent to search the bag, already knowing its contents. The officer engaged in parallel construction by officially stating that he asked explicit consent for a search, hiding the fact that he already conducted an unauthorized search in violation of the traveler's Fourth Amendment rights.

What other major sources of intelligence are government officials deliberately hiding through parallel construction? There are many: electronic surveillance, wiretaps, human sources, and foreign assets.[30] As described below, officials deliberately conceal the depth, scope, and operations of U.S. intelligence programs like Section 215 of the Patriot Act, Section 702 of the Foreign Intelligence Surveillance Act (FISA), and Executive Order (EO) 12333.

Abuse of Intelligence Authorities

Section 215 of the Patriot Act expired without reauthorization in 2020 – the House and Senate could not come to an agreement on a broader set of reforms to this Section of the Foreign Intelligence Surveillance Act.[31] Despite its expiration, a provision allowed officials to continue to use Section 215 for investigations that were ongoing prior to its expiration date, or, for offenses committed prior to that deadline.[i] Previously it was found that the NSA engaged in the bulk collection of American's phone metadata under Section 215. This indiscriminate search and seizure violated the Fourth Amendment.[32]

With a grandfathered-in clause like Section 215, one would expect the amount of surveillance conducted under its authority to decrease as cases existing prior to expiration were closed. This was not the case. The latest annual ODNI transparency report confirms that Section 215 thrives with 66,719 unique identifiers.[33]

EO 12333

EO 12333 contains no safeguards to prevent the collection of communications from Americans located outside of U.S. borders.[34] While an American cannot be targeted for collection individually without a court order, the contents of U.S. person's communications are "swept up" or "incidentally" collected in the course of lawful overseas investigations.[35] Many U.S. communications regularly transit through overseas routers, threatening the privacy of domestic Americans. According to a document declassified by ODNI, U.S. agencies may retain this collected data for up to 5 years.[36] EO 12333 is still shrouded in mystery and not subjected to proper judicial or congressional oversight. We only know this information thanks to whistleblowers like Edward Snowden and John Napier Tye.

O'Shaughnessy v. United States (2018) is an example of a publicly known case in which EO 12333 surveillance was likely deployed yet hidden from the defendants.[37] The O'Shaughnessy case involved a group of protesters that overtook the Malheur National Wildlife Refuge (MNWR) in Oregon in 2016. Twenty-six people were charged with being part of the occupation of the refuge. One of the protest-

i Sec. 102(b) of the USA PATRIOT Improvement and Reauthorization Act of 2005 includes the following exception: "With respect to any particular foreign intelligence investigation that began before the date on which the provisions referred to in paragraph (1) cease to have effect, or with respect to any particular offense or potential offense that began or occurred before the date on which such provisions cease to have effect, such provisions shall continue in effect."

ers, Joseph O'Shaughnessy, moved to withdraw his guilty plea on the basis that it was not knowing and voluntary, given the constraints placed on his attorneys to review discovery material "measured in gigabytes and terabytes." Furthermore, National Crime Information Center (NCIC) documents and an FBI search warrant executed at MNRW indicated that the protesters had been classified as "domestic terrorists."[38]

O'Shaughnessy's attorneys filed a motion to compel a notice of surveillance and for production of related discovery. Given his classification as a domestic terrorist, O'Shaughnessy's attorneys argued that it is highly likely he was the target of EO 12333 surveillance.[ii] In the motion they argue that "The government may have directly used EO 12333 to address the 'threats to national security' and may be withholding notice of such surveillance activities based on the flawed belief that if the government does not intend to the use the fruits of the surveillance against the defendants, then the government need not disclose the surveillance."[39]

O'Shaughnessy's case evidences parallel construction in the failure of prosecutors to disclose with proper notice their use of EO 12333 surveillance. Regardless of the nature of the protest, accessing the communications of participants under an unwarranted surveillance power is a blatant Fourth Amendment violation with potential First Amendment implications. O'Shaughnessy's case is representative of the larger problem that 42% of exonerations in 2016 were a result of official misconduct by both state and federal officials.[40]

FISA 702

Section 702 of the Foreign Intelligence Surveillance Act (FISA) is set to sunset by April 19, 2024, without Congressional renewal. Section 702, the "crown jewel" of surveillance authorities, grants intelligence agencies the power to surveil foreign nationals outside of the U.S.[41] As we have written previously, with the FISA Amendments Act of 2008 FISA pivoted from being focused on surveilling individuals to being primarily focused on mass surveillance.[42]

The FBI repeatedly violates Foreign Intelligence Surveillance Court (FISC) rules for handling Section 702-acquired data.[43] In 2018, the FBI conducted batch queries of over 70,000 people who had access to FBI systems, along with crime victims and people who provided tips to the agency.[44] According to a 2022 DNI report, the FBI queried the Section 702 database approximately 1.3 million times in 2020 and 3.4 million times in 2021.[45] A FISC opinion from 2022 noted with concern that the FBI misused Section 702 data to run searches on 19,000 congressional campaign donors, 133 Black Lives Matter protesters, as well as people outside the Capitol during the Jan 6. insurrection, and a sitting senator.[46]

FISA requires the government to notify U.S. citizens if it intends to use information derived from Section 702 surveillance against them in legal proceedings. Are these statutory notification requirements honored? Rarely – disclosures of Section 702 use are few and far in between. Up until 2013, no criminal defendant received notice of Section 702 surveillance despite the statutory requirement to do so.[iii] Non-disclosure of Section 702 surveillance precludes the criminal defendant from mounting a proper case in which they can review the evidence presented against them. Additionally, non-disclosure maintains the secretive nature of FISA 702 surveillance, thus protecting intelligence officials from public scrutiny. Without stronger notice and disclosure requirements enshrined into law, Section 702 continues to enable the illegal surveillance of US persons and people located in the US.[47]

According to an internal FBI memo dating back to 2003, FBI agents purposefully attempt to keep the surveillance technology and tactics they employ secretive.[48] The FBI goes so far as to hide this information from prosecutors because "There have been several instances of assistant U.S. attorneys becoming familiar with our technology, then resigning and becoming defense lawyers." These FBI internal policies promote parallel construction. If the initial evidence prompting an FBI investigation is not shared

ii See Part I of EO 12333, "General Purpose"

iii For statutory disclosure requirements of Section 702 derived information, see 50 US Code S. 1806 – Use of Information Section C: "Whenever the Government intends to enter into evidence...against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial, hearing, or other proceeding...disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information." The DOJ is responsible for these notices of surveillance. .

because it arises from an undisclosed surveillance method, then both the defense and prosecution are litigating without the benefits of discovery of the original evidence and the knowledge of whether it was legally collected. Since the surveillance is also concealed from the judge, they have no opportunity to rule on the legality of the collection method.

The case of Agron Hasbajrami is illustrative of the harms of parallel construction and Section 702 surveillance. Hasbajrami is a U.S. resident who was arrested at JFK airport in 2011 on his way to Pakistan. He was charged with providing material support to terrorists.

The government used Section 702 surveillance to build its case against Hasbajrami but it withheld this fact from his attorneys.[49] It was only after the 2013 Snowden Revelations that Hasbajrami and other defendants with similar civil cases against suspected undisclosed surveillance by the US government were eventually informed that they had been subjected to warrantless surveillance.[50]

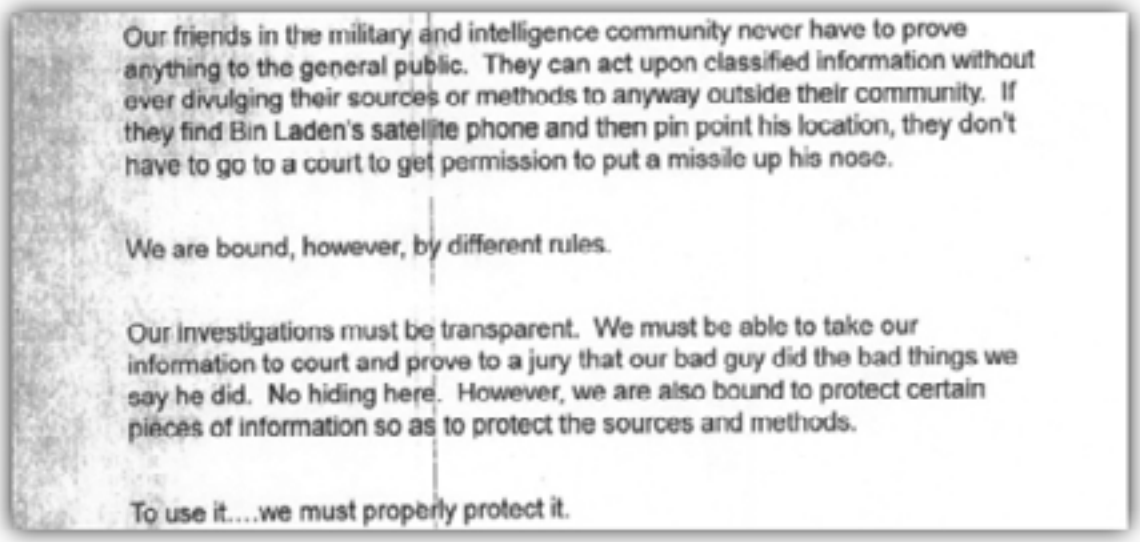
In 2019, the U.S. Court of Appeals for the Second Circuit issued a decision in *Hasbajrami*.[51] They ruled that the incidental collection of a U.S. citizen's communications that occur when the primary surveillance target is a non-U.S. based foreign national is permissible. However, they remanded the case to consider whether querying government databases for evidence related to a U.S. person could violate the Fourth Amendment.[52] The Second Circuit did recognize the privacy concerns that arise in the use of surveillance information in criminal cases.[53] Citing *Riley v. California*, they emphasized the need "for additional probable cause or reasonableness assessments to support a search of information or objects that the government has lawfully collected," and that programs like Section 702 "[begin] to look more like a dragnet, and a query more like a general warrant."[54]

Hasbajrami is a rare case because the defendant was eventually informed of his surveillance under Section 702. However, by the time of disclosure and prior to the 2nd Circuit's decision, Hasbajrami was already serving his 15-year prison sentence.[55] This highlights how parallel construction causes defendants who have not received proper disclosure of their surveillance to be unjustly sentenced for a crime because they could not challenge the evidence and the means by which it was procured.

Civil Liberties Issues and Parallel Construction

Parallel construction presents serious Fourth Amendment issues.

In the United States, the primary remedy for improper searches and seizures is the exclusionary rule, originating in *Weeks v. United States* (1914) and fully established in *Mapp v. Ohio* (1961).[56] Evidence illegally obtained is inadmissible and must be excluded from trial. This is important because it deters law enforcement officers from improper


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 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 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.

Slide from a DEA training presentation encouraging parallel construction.

conduct. When a defendant has knowledge that unlawful investigative techniques were used, they can ask for the evidence to be excluded and they may be able to have an attorney review the actual evidence in case it also exonerates them. Relatedly, information that is derived from excluded evidence is called the "fruit of the poisonous tree."[57] This is evidence that law enforcement derived from an original search or seizure in violation of the Fourth Amendment – information they otherwise would not have acquired.

There are many exceptions to the exclusionary rule, one of which is the independent source (IS) doctrine, which states that evidence initially obtained during an illegal search or seizure may be admissible if it is later obtained through a search or seizure compliant with constitutional protections.[58] Inevitable discovery (ID), a doctrine corollary to the independent source exception to the exclusionary rule, affords prosecutors the opportunity to prove by a preponderance of the evidence that in the absence of the illegal police conduct, officers would still have come across the evidence in the course of their investigation (See *Nix v. Williams* (1984)).[59]

To make an ID claim, prosecutors must prove the inevitability of finding the evidence. They may do this by referring to "hypothetical search warrants," a counterfactual world in which law enforcement would have obtained a judicially approved warrant if not for the circumstances. Legal scholars Tonja Jacobi and Elliot Louthen explain the issue with this speculative prosecutorial argument:[60]

> ...[M]any circuits flip the requirement of ex ante review into an ex-post presumption of constitutionality... Even when law enforcement fails to comply with some element of the warrant process at the outset, ID gives the state an opportunity to argue it could have and would have obtained proper judicial sign-off. In this way, the state can admit otherwise illegally obtained evidence through a hypothetical search warrant in the counterfactual world that inevitable discovery affords, giving the state a second bite at the apple.

The Supreme Court's Nix decision attempted to develop a test that struck a balance between deterring police misconduct and not hampering police work when assessing ID claims. However, because ID claims depend on police testimony, who have the benefit of hindsight, it is difficult to verify how accurate a counterfactual claim is. Officers can rationalize their wrongful conduct, which is "always post hoc, subject to unintentional revision, or worse, intentional coaching geared toward inevitable discovery's requirements."

ID claims can be powerful tools for law enforcement officers or intelligence officials engaging in parallel construction. ID is a safety valve for officials intent on hiding the original sources of their investigations. An ID claim can bolster the parallel construction process by providing law enforcement the opportunity to rationalize any wrongful conduct that may occur in the process of an investigation. ID is another layer of concealment in cases made opaque by parallel construction.

It is important to emphasize that parallel construction and ID are not the same. ID is a legally recognized argument that Circuit courts have evaluated since the Nix decision. There are many different tests and assessments that Circuit justices have employed to determine if an ID claim can be made. On the other hand, parallel construction is indisputably an illegal tactic deployed to build cases and secure convictions. However, both have a corrosive effect on the Fourth Amendment.[iv]

Not only does parallel construction undermine the Fourth Amendment, but it also runs contrary to the protections enshrined in the Sixth Amendment, which guarantees the rights of criminal defendants to know who their accusers are and the nature of the charges and to see the evidence against them. Without proper notice, criminal defendants are left in the dark as to where the evidence levied against them originates. The Sixth Amendment also guarantees effective assistance of counsel, whether that attorney be privately retained, or court appointed. Assistance of counsel cannot be considered "effec-

iv For further jurisprudence on the exclusionary rule, see Kyles v. Whitley (1995): "First, favorable evidence is material, and constitutional error results from its suppression by the government, if there is a "reasonable probability" that, had the evidence been disclosed to the defense, the result of the proceeding would have been different. Thus, a showing of materiality does not require demonstration by a preponderance that disclosure of the suppressed evidence would have resulted ultimately in the defendant's acquittal."

tive" if they are deprived of the totality of evidence levied against the defendant (See *Strickland v. Washington* (1984)). Therefore, cases of parallel construction likely fall into this category.[61]

Parallel construction precludes judges from evaluating whether emerging surveillance technology and tactics employed by the government adhere to the Constitution and statutory protections.[62] New surveillance technology, like facial recognition cameras, raise legal concerns. There are now multiple instances in which facial recognition technology (FRT) has incorrectly identified someone as a criminal suspect. Those wrongly identified were Black people, whom FRT has trouble accurately identifying.[63] To borrow an example from Human Rights Watch: if the government were to identify a criminal suspect using a flawed FRT system they did not want to disclose in court records, they could engage in parallel construction by sending an informant to talk to the suspect and claim that this conversation was the start of the investigation. In this scenario, judges would not be able to assess the impact of nascent surveillance technology on Americans' civil liberties.[64]

How to fix parallel construction

Recent efforts in Congress to limit government surveillance powers in general have also included specific language addressing parallel construction. We and many other civil liberties organizations have endorsed this language, and it could easily form the basis of a stand-alone bill on the subject as needed, if not passed in Congress.

The Government Surveillance Reform Act (GSRA)

Representatives Zoe Lofgren (D-CA, 18th District), Warren Davidson (R-OH, 8th District) and Senators Ron Wyden (D-OR) and Mike Lee (R-UT), along with a privacy and civil liberties coalition of more than 30 groups, of which we are a member, have proposed the Government Surveillance Reform Act of 2023.[65] The GSRA is a comprehensive reform proposal that, most significantly, would codify a warrant requirement for U.S. person queries of data collected under FISA Section 702 and Executive Order 12333. It also strengthens statutory limits placed on government surveillance under the Electronic Communications Privacy Act of 1986.[66]

Below is a section-by-section breakdown of each relevant section of the GSRA and how its provisions have the potential to stop parallel construction in future cases:

SECTION 101 of the GSRA prohibits warrantless queries of U.S. persons' communication. It outlines the process necessary for obtaining a judicially approved criminal warrant or a Title I FISA order to obtain Section 702 data. It reads: "...no officer or employees of the United States may conduct a query of information acquired under this section in an effort to find communications or information the compelled production of which would require a probable cause warrant if sought for law enforcement purposes in the United States..." Section 302 effectively proposes the same restrictions but applied to surveillance conducted under EO 12333.

Section 101 is the bedrock principle of the GSRA. By limiting U.S. person queries through stricter procedural requirements in line with the Fourth Amendment, there would be many less opportunities for intelligence or law enforcement agents to query Section 702 data, for example, to find leads or evidentiary trails they intend to hide later.

"The GSRA is a once-in-a-generation opportunity for comprehensive surveillance reform."

SECTION 202 amends FISA to include the required disclosure of relevant information for those surveilled under Section 702. FISA applications to FISC must include all relevant information, including potentially exculpatory information or information that would raise doubts or call the accuracy of the case into question.

Cases of parallel construction are built on an asymmetry of information between intelligence or law enforcement officials and criminal defendants, whose cases are damaged by withheld information. Section 202 would eliminate the ability of officials to do this. In sum, officials can longer lie to judges, either outright or by omission.

SECTION 204 clarifies proper notice requirements for FISA-derived information and evidence. Any information that would not have been found if not for electronic surveillance, a physical search, or other means of surveillance "regardless of any claim that the information or evidence is attenuated from the surveillance... or was subsequently reobtained through other means" must be disclosed with proper notice.

This provision explicitly eliminates parallel construction without employing the term. It precludes law enforcement from building alternative evidentiary chains that would be legally admissible in a court of law without disclosing the original source of the evidence in their possession.

SECTION 210 establishes grounds for a U.S. person to file a civil action in response to the "acquisition, copying, querying, retention, access, or use" of information acquired under FISA if the person has a reasonable basis to believe that their rights have been or will be violated. This provision would allow a person to receive damages in known instances of parallel construction, deemed illegal by Sections 202 and 204.

Even more impactful in Section 210 is a provision that abrogates the state secrets privilege. The state secrets privilege is a common law evidentiary privilege that allows the head of a relevant government agency to prevent the discovery of certain information if it would prove to be a "reasonable danger" to national security.[67] The Classified Information Procedures Act (CIPA) is the statute that outlines how information is withheld from criminal defendants (it also applies to civil cases). State secrets privilege is regularly abused by intelligence officials to hide key information necessary for defendants to mount a defense, especially when seeking to suppress illegally obtained evidence.[68] The government evoked state secrets in *Wikimedia v. NSA*, wherein the constitutionality of the NSA's Upstream surveillance program was challenged.[69]

The GSRA is a once-in-a-generation opportunity for comprehensive surveillance reform. It is a strong policy solution to diminish opportunities for parallel construction.

The Protect Liberty and End Warrantless Surveillance Act (PLEWSA)

The Protect Liberty and End Warrantless Surveillance Act (PLEWSA), H.R. 6570, is a bipartisan bill passed out of the House Judiciary Committee 35-2.[70] It's sponsored by Rep. Andy Biggs (R, AZ-5) and its co-sponsors include Reps. Jerry Nadler, Jim Jordan, Pramila Jayapal, and Sara Jacobs, amongst others. PLEWSA is endorsed by Restore the Fourth and our civil liberties coalition partners.

PLEWSA's key reforms include:

- A warrant requirement for searches of U.S. persons communications collected under Section 702.

- The inclusion of the Lee-Leahy Amendment (See Section 5), which strengthens the role of amici curiae and requires their expertise in any case before the Foreign Intelligence Surveillance Court (FISC) that involves novel or significant privacy and civil liberties issues. Amici are also required in sensitive cases that involve religious groups, journalists, or groups participating in First Amendment protected protest.[71]

- Provisions from the Fourth Amendment Is Not for Sale Act (See Section 18), which prohibits law enforcement and intelligence agencies from purchasing location and other sensitive information in an end-run around the Fourth Amendment (closing the "Data Broker Loophole").[72]

PLEWSA also contains key provisions that, if enacted, would prevent intelligence and law enforcement officials from engaging in parallel construction. Below is a section-by-section breakdown of how PLEWSA corrects parallel construction:

PLEWSA Section 2(b) prohibits warrantless queries of U.S. persons communications and communications from persons reasonably believed to be in the U.S. at the time of the communication or creation of information. In addition to the warrant requirement, PLEWSA places strict limitations on how and where information retrieved pursuant to an authorized query is used. As outlined in Section 2(B)(ii)(I), information derived from an approved query may not be "…used, received in evidence, or otherwise disseminated in any investigation, trial, hearing, or other proceeding in or before any court [or] grand jury" except in cases directly related to the threat that prompted the query. This clause has the potential to stop officials from engaging in parallel construction by limiting the contexts in which they can use FISA 702 derived information.

Section 3(2) of PLEWSA prohibits 702-derived information from being introduced as evidence against U.S. persons in criminal or civil investigations. There are exceptions to this rule for certain terrorism cases, as defined in the 2001 Patriot Act. PLEWSA's criminal, civil, and administrative penalties for intentional misuse of 702 data or violation of querying procedures, when paired with Section 3(2), deter officials from hiding the origins of their investigations. PLEWSA outright bans law enforcement from initiating investigations of U.S. persons with FISA query data.

Sections 9 and 11 of PLEWSA contains multiple reporting provisions. The Director of the FBI, the Attorney General for the Department of Justice, and Office for the Director of National Intelligence must produce compliance reports annually. These reports must indicate the quantity of query violations committed by personnel, and document updated query protocols and rules. While these transparency provisions are not a direct fix, the key issue with parallel construction cases is information asymmetry – intelligence officials bury the truth behind their investigations. Transparency provisions in PLEWSA would clue civil liberties watchdogs and attorneys into how the IC is using FISA 702 data, and potentially help us determine if parallel construction is being deployed.

PLEWSA Section 901 ensures that FISC issued court orders to conduct queries are based on applications that contain accurate, complete information. Applications must include a file documenting each factual assertion made by the agency with supporting documentation. Officers must also include any information that calls into question the accuracy or reasonableness of their findings, including information that questions the reliability of a human source. This is similar to Section 202 of the GSRA – officials would be barred from lying to judges, either outright or by omission.

Started in 2013, Restore The Fourth stands against mass government surveillance. We seek to strengthen the Fourth Amendment and fight back against all programs that encroach on it through educating the public, lobbying elected officials, and supporting grassroots organizers across the country.

For more information, please visit our website: https://restorethe4th.com/

References

1. "Wray Plays Dumb on Parallel Construction FISA Abuse," Daily Torch (blog), July 13, 2023, https://dailytorch.com/2023/07/wray-plays-dumb-on-parallel-construction-fisa-abuse/; "Oversight of the Federal Bureau of Investigation | House Judiciary Committee Republicans," July 5, 2023, http://judiciary.house.gov/committee-activity/hearings/oversight-federal-bureau-investigation-0.

2. "Parallel Construction," Carmichael, Ellis, & Brock PLLC, accessed February 25, 2024, https://www.carmichaellegal.com/parallel-construction.

3. Peter Van Buren, "Parallel Construction: Unconstitutional NSA Searches Deny Due Process," HuffPost, July 21, 2014, https://www.huffpost.com/entry/parallel-construction-unc_b_5606381.

4. United States v. Alverez Tejeda, No. 06-30289 (US Court of Appeals, Ninth Circuit June 8, 2007).

5. Trevor Aaronson, "Welcome to Law Enforcement's 'Dark Side': Secret Evidence, Illegal Searches, and Dubious Traffic Stops," The Intercept, January 9, 2018, https://theintercept.com/2018/01/09/dark-side-fbi-dea-illegal-searches-secret-evidence/.

6. "Criminal Law. Fourth Amendment. Ninth Circuit Upholds Car Seizure through Staged Accident and Theft. United States v. Alverez-Tejeda, 491 F.3d 1013 (9th Cir. 2007)," Harvard Law Review 121, no. 7 (2008): 1930–36.

7. "U.S. v. ALVEREZ-TEJEDA, 491 F.3d 1013 | 9th Cir., Judgment, Law, Casemine.Com," https://www.casemine.com, accessed February 25, 2024, https://www.casemine.com/judgement/us/59146dfaadd7b0493432d28d.C

8. "Kurbanov Sentenced to 25 Years in Prison," US Attorney's Office, District of Idaho, January 7, 2016, https://www.justice.gov/usao-id/pr/kurbanov-sentenced-25-years-prison.

9. Trevor Aaronson, "NSA Secretly Helped Convict Defendants in U.S. Courts, Classified Documents Reveal," The Intercept, November 30, 2017, https://theintercept.com/2017/11/30/nsa-surveillance-fisa-section-702/.'

10. Glenn Greenwald, Ewen MacAskill, and Laura Poitras, "Edward Snowden: The Whistleblower behind the NSA Surveillance Revelations," The Guardian, June 11, 2013, sec. US news, https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance; T. C. Sottek, "Everything You Need to Know about PRISM," The Verge, July 17, 2013, https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet.

11. Sarah St.Vincent, "Dark Side: Secret Origins of Evidence in US Criminal Cases" (Human Rights Watch, January 9, 2018), https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases.

12. Whren v. United States, 517 U.S. 806 (1996), No. 95-5841 (US Court of Appeals, District of Columbia June 10, 1996).

13. John Shiffman and Kristina Cooke, "Exclusive - U.S. Directs Agents to Cover up Program Used to Investigate Americans," Reuters, August 5, 2013, sec. World, https://www.reuters.com/article/idUSBRE9740HP/.

14. John Shiffman and David Ingram, "Exclusive: IRS Manual Detailed DEA's Use of Hidden Intel Evidence," Reuters, August 7, 2013, sec. United Kingdom, https://www.reuters.com/article/idUSBRE9761B0/.

15. Ibid.

16. "Border Searches," Justia Law, February 28, 2024, https://law.justia.com/constitution/us/amendment-04/19-border-searches.html.

17. Aaron Keller, "'Dark Side' Federal Unit Feeds Possibly Illegal Tips to Local Cops, Report Says," Law & Crime, January 9, 2018, https://lawandcrime.com/high-profile/dark-side-federal-unit-feeds-possibly-illegal-tips-to-local-cops-report-says/.

18. "New Documents Reveal NSA Improperly Collected Americans' Call Records Yet Again," American Civil Liberties Union, June 26, 2019, https://www.aclu.org/press-releases/new-documents-reveal-nsa-improperly-collected-americans-call-records-yet-again.

19. Scott Shane and Colin Moynihan, "Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s - The New York Times," The New York Times, September 1, 2013, https://web.archive.org/web/20170202235201/https:/www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html.

20. Dave Maass, "Before and After: What We Learned About the Hemisphere Program After Suing the DEA," Electronic Frontier Foundation, December 19, 2018, https://www.eff.org/deeplinks/2018/12/and-after-what-we-learned-about-hemisphere-program-after-suing-dea.

21. "A Review of the Drug Enforcement Administration's Use of Administrative Subpoenas to Collect or Exploit Bulk Data" (Office of the Inspector General, U.S. Department of Justice, March 2019), https://oig.justice.gov/reports/2019/o1901.pdf.

22. Kenneth Lipp, "AT&T Is Spying on Americans for Profit," The Daily Beast, April 13, 2017, https://www.thedailybeast.com/atandt-is-spying-on-americans-for-profit.

23. Dell Cameron, "Secretive White House Surveillance Program Gives Cops Access to Trillions of US Phone Records," WIRED, November 20, 2023, https://www.wired.com/story/hemisphere-das-white-house-surveillance-trillions-us-call-records/; Restore The Fourth, "DAS - The Secret Surveillance Program That Gives Cops Access to Trillions of Phone Records," Restore the Fourth, November 21, 2023, https://restorethe4th.com/das-the-secret-surveillance-program-that-gives-cops-access-to-trillions-of-phone-records/.

24. Carpenter v. United States, No. 16-402 (U.S. Supreme Court 2018).

25. Barton Gellman, "Inside the NSA's Secret Tool for Mapping Your Social Network," WIRED, May 24, 2020, https://archive.is/R8KU4; American Civil Liberties Union (ACLU) v. James R. Clapper, No. 14-42-cv (US Court of Appeals, Second Circuit May 7, 2015).

26. "Synopsis of the Hemisphere Project," https://www.nytimes.com/interactive/2013/09/02/us/hemisphere-project.html.

27. Shawn Musgrave, "DEA Teaches Agents to Recreate Evidence Chains to Hide Methods," MuckRock, February 3, 2014, https://www.muckrock.com/news/archives/2014/feb/03/dea-parallel-construction-guides/.

28. "Drug Enforcement Administration Lesson Plan - Handling Sensitive Information," June 4, 2007, https://www.documentcloud.org/documents/1011382-responsive-documents.html#document/p9., P. 161.

29. United States v. Grobstein, No. 13 CR 0663 MV (US District Court for the District of New Mexico April 26, 2013).

30. Brian Pori and Sarah St. Vincent, "Parallel Construction: How to Discover the Government's Undisclosed Sources of Evidence" (Webinar, National Association of Criminal Defense Lawyers (NACDL), May 23, 2018), https://www.nacdl.org/Media/Parallel-Construction-Discover-Govt-Evidenc-Source.

31. India McKinney, "Section 215 Expired: Year in Review 2020," Electronic Frontier Foundation, December 29, 2020, 215, https://www.eff.org/deeplinks/2020/12/section-215-expired-year-review-2020.

32. Jake Laperruque, "The History and Future of Mass Metadata Surveillance," POGO, June 11, 2019, https://www.pogo.org/analysis/the-history-and-future-of-mass-metadata-surveillance.

33. "Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities" (Office of the Director of National Intelligence, April 2022), https://www.dni.gov/files/CLPT/documents/2022_ASTR_for_CY2020_FINAL.pdf.

34. "Executive Order 12333," 46 FR 59941 § (1981), https://web.archive.org/web/20220203121403/https:/www.archives.gov/federal-register/codification/executive-order/12333.html.

35. Faiza Patel, Elizabeth Goitein, and Amos Toh, "Overseas Surveillance in an Interconnected World" (New York University School of Law: The Brennan Center for Justice, March 16, 2016), https://www.brennancenter.org/our-work/research-reports/overseas-surveillance-interconnected-world.

36. "Legal Compliance and U.S. Persons Minimization Procedures" (National Security Agency (NSA), Signals Intelligence Directive (SID), January 25, 2011), https://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf.

37. Laura Graser, O'Shaughnessy v. U.S. (U.S. Court of Appeals, Ninth Circuit December 13, 2018).

38. Defendant's Memorandum In Support of Motion to Compel Notice of Surveillance and For Production of Related Discovery, No. 3:16-cr-00061-MO (May 11, 2016).

39. Ibid, 7.

40. Henry Gass, "Cliven Bundy Case: How Big a Problem Is Prosecutorial Misconduct?," Christian Science Monitor, January 11, 2018, https://www.csmonitor.com/USA/Justice/2018/0111/Cliven-Bundy-case-How-big-a-problem-is-prosecutorial-misconduct; "Exonerations in 2016" (Newkirk Center for Science and Society: The National Registry of Exonerations, March 7, 2017), https://www.law.umich.edu/special/exoneration/documents/exonerations_in_2016.pdf.

41. Dell Cameron, "Top US Spies Meet With Privacy Experts Over Surveillance 'Crown Jewel,'" WIRED, September 8, 2023, https://www.

wired.com/story/section-702-privacy-meeting/.

42. "FISA," Restore the Fourth, accessed February 26, 2024, https://restorethe4th.com/issues/fisa/.

43. "Timeline of Selected Legal and Constitutional Violations in Programs Operated under Section 702," accessed February 26, 2024, https://s3.amazonaws.com/demandprogress/documents/Sec._702_Violations_Handout.pdf.

44. "FISA Section 702 Issue Brief: The FBI's Misuse of FISA 702 In the Past Indicates That Its Procedural Reforms Will Not Break Its Pattern of Misuse In the Future" (Center for Democracy and Technology, July 2023), https://cdt.org/wp-content/uploads/2023/07/CDT-Issue-Brief-Internal-Procedures-Will-Not-Fix-FISA-702.pdf.

45. "Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities."

46. Rudolph Contreras, Memorandum Opinion and Order (U.S. Foreign Intelligence Surveillance Court April 21, 2022); Maggie Miller, "FBI Misused Surveillance Authorities to Investigate Black Lives Matter Protesters," POLITICO, May 19, 2023, https://www.politico.com/news/2023/05/19/fbi-surveillance-black-lives-matter-protesters-00097924.

47. Patrick C. Toomey, "Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance — Again?," Just Security, December 11, 2015, https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again/.

48. 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/.

49. "United States v. Hasbajrami," Electronic Frontier Foundation, August 29, 2018, https://www.eff.org/cases/united-states-v-hasbajrami.

50. Ewen MacAskill et al., "NSA Files Decoded: Edward Snowden's Surveillance Revelations Explained," The Guardian, November 1, 2013, http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded.

51. United States v. Hasbajrami, No. 15-2684 (U.S. Court of Appeals, Second Circuit December 18, 2019).

52. Jacques Singer-Emery, "The Second Circuit Rules in United States v. Hasbajrami," Lawfare, January 7, 2020, https://www.lawfaremedia.org/article/second-circuit-rules-united-states-v-hasbajrami.

53. Alan Butler, Jake Wiener, and Chris Baumohl, "EPIC Comments: PCLOB Investigation of Section 702 Surveillance," EPIC - Electronic Privacy Information Center (blog), November 4, 2022, https://epic.org/documents/epic-comments-pclob-investigation-of-section-702-surveillance/.

54. Riley v. California, No. 13-132 (U.S. Supreme Court April 29, 2014).

55. "United States v. Hasbajrami — Second Circuit Opinion," American Civil Liberties Union, accessed February 26, 2024, https://www.aclu.org/legal-document/united-states-v-hasbajrami-second-circuit-opinion.

56. Weeks v. United States, No. 461 (U.S. Supreme Court February 24, 1914); Mapp v. Ohio, 367 U.S. 643 (1961) (U.S. Supreme Court June 19, 1961).

57. Robert M. Pitler, "'The Fruit of the Poisonous Tree' Revisited and Shepardized," California Law Review 56, no. 3 (May 1968): 579, https://doi.org/10.2307/3479264.

58. "Exclusionary Rule," Cornell Law School - Legal Information Institute, November 2022, https://www.law.cornell.edu/wex/exclusionary_rule.

59. "Inevitable Discovery Rule," Cornell Law School- Legal Information Institute, May 2022, https://www.law.cornell.edu/wex/inevitable_discovery_rule; Nix v. Williams (U.S. Supreme Court June 11, 1984).

60. Tonja Jacobi and Elliot Louthen, "The Corrosive Effect of Inevitable Discovery on the Fourth Amendment," University of Pennsylvania Law Review 171, no. 1 (2022), https://doi.org/10.2139/ssrn.4035683.

61. Strickland v. Washington, No. 82-1554 (U.S. Court of Appeals for the Eleventh Circuit May 14, 1984).

62. Tim Cushing, "Report Shows US Law Enforcement Routinely Engages In Parallel Construction," Techdirt, January 22, 2018, https://www.techdirt.com/2018/01/22/report-shows-us-law-enforcement-routinely-engages-parallel-construction/.

63. Natasha Johnson and Thaddeus Johnson, "Police Facial Recognition Technology Can't Tell Black People Apart," Scientific Amer-

ican, May 18, 2023, https://www.scientificamerican.com/article/police-facial-recognition-technology-cant-tell-black-people-apart/.

64. St.Vincent, "Dark Side: Secret Origins of Evidence in US Criminal Cases."

65. Zoe Lofgren et al., "Government Surveillance Reform Act of 2023," Pub. L. No. H.R. 6262/S.R 3234 (2023).

66. "Electronic Communications Privacy Act of 1986," Pub. L. No. 99–508, 2510 (1986), https://www.justice.gov/jmd/ls/electronic-communications-privacy-act-1986-pl-99-508.

67. Harry Graver, "The Classified Information Procedures Act: What It Means and How It's Applied," Lawfare, November 20, 2017, https://www.lawfaremedia.org/article/classified-information-procedures-act-what-it-means-and-how-its-applied.

68. Bennett Cyphers, "Privileged Methods, Parallel Construction: How Government Secrecy Undermines the Fourth Amendment," Berkeley Journal of Criminal Law, January 17, 2023, https://www.bjcl.org/blog/privileged-methods-parallel-construction-how-government-secrecy-undermines-the-fourth-amendment.

69. "Wikimedia v. NSA - Challenge to Upstream Surveillance," American Civil Liberties Union (blog), February 21, 2023, https://www.aclu.org/cases/wikimedia-v-nsa-challenge-upstream-surveillance.

70. Andy Biggs, "Protect Liberty and End Warrantless Surveillance Act of 2023," Pub. L. No. H.R.6570 (2023), https://www.congress.gov/bill/118th-congress/house-bill/6570.

71. "Lee-Leahy Introduce Bipartisan FISA Reform Bill," Mike Lee US Senator for Utah, March 9, 2020, https://www.lee.senate.gov/2020/3/lee-leahy-introduce-bipartisan-fisa-reform-bill.

72. Warren Davidson, "Fourth Amendment Is Not For Sale Act," Pub. L. No. H.R. 4639 (2023), https://www.cbo.gov/publication/59756; Noah Chauvin, "New Legislation Would Close a Fourth Amendment Loophole," Brennan Center for Justice, July 6, 2023, https://www.brennancenter.org/our-work/analysis-opinion/new-legislation-would-close-fourth-amendment-loophole.

73. "EPIC Statement on Reforming Intelligence and Securing America Act (RISAA)," EPIC - Electronic Privacy Information Center (blog), February 13, 2024, https://epic.org/epic-statement-on-reforming-intelligence-and-securing-america-act-risaa/.

74. Mark R. Warner, "FISA Reform and Reauthorization Act of 2023," Pub. L. No. S.3351 (2023), https://www.congress.gov/bill/118th-congress/senate-bill/3351/text.

75. "FISA 'Reform' and Reauthorization Act: The Biggest Expansion in Government Surveillance Since the Patriot Act," Brennan Center for Justice, December 11, 2023, https://www.brennancenter.org/our-work/research-reports/fisa-reform-and-reauthorization-act-biggest-expansion-government.