NACDL FOURTH AMENDMENT CENTER

Practice Advisory: Law Enforcement Access to Bulk Money Transfer Data

I. Introduction

Since 2010, law enforcement agencies in the United States have had direct access to an increasing volume of bulk data about people's wire transfer transactions. As Senator Ron Wyden explained when revealing the previously secret program, law enforcement has been "operating an indiscriminate and bulk surveillance program that swept up millions of financial records about Americans."[1]

At the core of the program is a database containing records of virtually every money transfer for more than $500 sent to, from, or within Arizona, California, New Mexico, Texas, or Mexico, as well as transactions from anywhere in the U.S. to 23 other countries and territories.[2] For example, money transfers exceeding $500 sent from Mexico to New York, from one party in Arizona to another party in Arizona, or from Oregon to California, are tracked in the database, as are transactions between Nebraska and Spain, or Florida and Panama. Thousands of law enforcement officers from hundreds of agencies across the country have the ability to directly query the database—which contains records of more than 150 million money transfers—without any legal process or judicial oversight.

This practice advisory aims to: 1) explain what was involved in this bulk money transfer surveillance program; and 2) provide defense counsel with potential challenges to it.

II. Background

In 2006, the Arizona Attorney General ("AG") issued a subpoena under a state anti-racketeering investigative statute to Western Union, seeking records of "any wire-transfers made in an amount of $300 or more to any location in Sonora, Mexico from any Western Union location worldwide for a three-year period."[3] But a state appellate court held the scope of the AG's investigation was

[1] Letter from U.S. Senator Ron Wyden to Joseph V. Cuffari, Inspector Gen., Dep't of Homeland Sec. (Mar. 8, 2022), https://www.wyden.senate.gov/imo/media/doc/DHS%20IG%20ICE_HSI%20data%20complaint%20final.pdf.

[2] Those 23 countries and territories include: Argentina, Bahamas, Barbados, Bolivia, Canada, China, Colombia, Costa Rica, Curaçao, the Dominican Republic, Ecuador, France, Hong Kong, Malaysia, Panama, Peru, Spain, St. Martin/St. Maarten, Thailand, Tortola (British Virgin Islands), Ukraine, the U.S. Virgin Islands, and Venezuela. *See* Letter from U.S. Senator Ron Wyden to Michael E. Horowitz, Inspector Gen., Dep't of Justice (Jan. 18, 2023), https://www.wyden.senate.gov/imo/media/doc/Wyden%20letter%20to%20DOJ%20IG%20money%20transfer%20letter%201.18.23.pdf.

[3] State *ex rel.* Goddard v. W. Union Fin. Servs., Inc., 166 P.3d 916, 917 (Ariz. Ct. App. 2007).

"not authorized by Arizona law" and amounted to a request for "limitless" investigative power.[4] Subsequently, in 2010, the Arizona AG and Western Union reached a settlement to resolve a lawsuit brought by the AG under a state anti-money laundering law.[5] The settlement required that Western Union turn over bulk transaction data for all money transfers over $500 made to or from Arizona, California, New Mexico, Texas, or Mexico.[6] Western Union and the Arizona AG entered into a second settlement agreement in 2014, extending the bulk data-sharing arrangement to 2019.[7] The second settlement established a new 501(c)(3) nonprofit organization, the Transaction Record Analysis Center ("TRAC"), to "facilitate law enforcement access to the bulk data."[8] The agreement required Western Union to pay hundreds of thousands of dollars to fund TRAC's budget.

From February 2010 to July 2019, "Western Union provided millions of records . . . to the Arizona AG and TRAC pursuant to the settlement agreement," including "all records of money transfers above $500, to or from Arizona, California, New Mexico, Texas and Mexico."[9] But Western Union was not the only money transfer company to disclose customer records to TRAC—over time, "dozens of other money transfer businesses also provided TRAC with similar bulk transaction data."[10] TRAC documents indicate that as of early 2021, there were "28 different [money service businesses] providing data to the TRAC database," which, at that time, amounted to "over 145 million records."[11] And while initial reporting suggested those companies were providing records to TRAC "voluntarily," records disclosed in response to a public records request from the American Civil Liberties Union to the Arizona AG's office revealed the AG has been sending prospective, annual bulk records subpoenas to several money transfer companies, directing each to produce customer data on an ongoing basis over the next year.[12] In response to the ACLU public records request, the AG produced 140 of these subpoenas, issued between 2014 and 2021 to 18 money transfer companies.[13] By early 2023, TRAC's database had swollen to over 150 million wire transfer records.[14] Moreover, TRAC provided access to the money-

[4] *Id.* at 920, 926; *see also id.* at 927 (vacating the trial court's enforcement of the subpoena because "the breadth of the Attorney General's request was not reasonable in light of the justification offered for it").
[5] Settlement Agreement, State *ex rel.* Goddard v. W. Union Fin. Servs., Inc., 166 P.3d 916 (Ariz. Ct. App. 2007) (No. 1 CA-CV 06-0700 Feb. 11, 2010), https://www.azag.gov/sites/default/files/docs/criminal/border-security/swbamla/State_of_Arizona_v_Western_Union_Settlement_Agreement.pdf.
[6] *Id.* at 6, 11; *see also* Letter from Sen. Wyden, *supra* note 1.
[7] Stipulated Mot. for Approval of Amend. to Settlement Agreement, State *ex rel.* Horne v. W. Union Fin. Servs., Inc., No. CV 2010-005807 (Ariz. Super. Ct. Jan. 31, 2014), https://azag.gov/sites/default/files/2018-06/201402030745.pdf.
[8] Letter from Sen. Wyden, *supra* note 1.
[9] *Id.*
[10] *Id.*
[11] TRANSACTION RECORD ANALYSIS CTR., INC., MINUTES OF A REGULAR ANNUAL TELECONFERENCE MEETING OF THE BOARD OF DIRECTORS OF THE TRANSACTION RECORD ANALYSIS CENTER, INC. ("TRAC") 2 (2021), https://www.aclu.org/2021-1-15-minutes-board-meeting.
[12] *See* Fikayo Walter-Johnson & Nathan Freed Wessler, *How the Arizona Attorney General Created a Secretive, Illegal Surveillance Program to Sweep up Millions of Our Financial Records*, ACLU (Jan. 18, 2023), https://www.aclu.org/news/privacy-technology/how-the-arizona-attorney-general-created-a-secretive-illegal-surveillance-program.
[13] *See Arizona AG Money Transfer Surveillance FOIA Database*, ACLU, https://www.aclu.org/foia-collection/arizona-ag-money-transfer-surveillance-foia-database (last updated Jan. 18, 2023).
[14] Dustin Volz & Byron Tau, *Little-Known Surveillance Program Captures Money Transfers Between U.S. and More than 20 Countries*, WALL ST. J. (Jan. 18, 2023), https://www.wsj.com/articles/little-known-surveillance-

transfer data to "hundreds of federal, state and local law-enforcement agencies, who could mine the data for leads without being required to issue a warrant."[15] The ACLU obtained a list of more than 700 law enforcement agencies and field offices that have been given direct log-in access to the TRAC database.[16]

After the second settlement with Western Union expired in 2019, Arizona's AG sought assistance from the Department of Homeland Security ("DHS")—via the Phoenix Field Office of Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI")—"to compel [Western Union] to continue sharing data."[17] Between July 2019 and January 2022, the HSI Phoenix Field Office issued six customs summonses to Western Union for continued provision of the bulk data. It also began issuing summonses to a second money transfer company, Maxitransfers Corporation ("Maxi"), starting in 2021. The HSI summonses were issued under the authority of 19 U.S.C. § 1509, an administrative subpoena statute conferring limited authority to request records related to importation of merchandise.

Rather than seek evidence relevant to the investigation of particular customs-related crimes as the statute contemplates, ICE used the summonses to *prospectively* direct "the compan[ies] to transmit [bulk] records of money transfers directly to TRAC *for the next six months*."[18] Additionally, HSI's San Juan field office was issuing summonses to at least two other money transfer companies, Euronet and Viamericas, for bulk data on transfers from anywhere in the United States to 22 countries, and to Maxi for records on transfers from 21 U.S. states to Colombia, the Dominican Republic, Venezuela, and the U.S. Virgin Islands.[19] The records likely included the senders' names, addresses, and some type of identification number, along with the recipients' names and addresses.[20]

After learning about this program in 2021, Senator Ron Wyden contacted HSI to request a briefing in January 2022. In response, HSI "immediately terminated" its summonses under the customs statute.[21] However, other money transfer companies have apparently continued providing bulk records to TRAC in response to the Arizona AG's subpoenas. On March 8, 2022, Senator Wyden sent a letter to the DHS Inspector General, requesting an investigation of this "indiscriminate and bulk surveillance program."[22] And in January 2023, after learning the DEA and FBI were also sending subpoenas to money transfer companies and compelling them to send

---

program-captures-money-transfers-between-u-s-and-more-than-20-countries-11674019904. The volume of other companies' transfers to TRAC means that Western Union's records account for just three percent of TRAC's database. Michelle Hackman & Dustin Volz, *Secret Surveillance Program Collects Americans' Money-Transfer Data, Senator Says*, WALL ST. J. (Mar. 8, 2022), https://www.wsj.com/articles/secret-surveillance-program-collects-americans-money-transfer-data-senator-says-11646737201.

[15] Hackman & Volz, *supra* note 14.

[16] *See* E-mail from Richard Lebel, Exec. Dir., Transaction Record Analysis Ctr., to Carol Keppler (May 2, 2022, 2:17 PM), https://www.aclu.org/2022-05-02-trac-email-re-data-policy-mou-agency-list.

[17] *Id.*

[18] Letter from Sen. Wyden, *supra* note 1 (emphasis added).

[19] Letter from Sen. Wyden, *supra* note 2.

[20] *See* Hackman & Volz, *supra* note 14.

[21] Letter from Sen. Wyden, *supra* note 1.

[22] *Id.*

bulk records to TRAC, Senator Wyden wrote to the Department of Justice Inspector General, seeking an investigation of violations of law or policy by agencies within the DOJ.[23]

This program amounts to governmental bulk surveillance sweeping in individuals simply because they wired more than $500 using a money transfer company. And because of unequal access to traditional banking services, this surveillance program has a disproportionate effect on immigrants, people of color, and poor people.[24]

If there is any possibility your client was involved in a money transfer that may have contributed to the government's investigation (e.g., a money transfer for more than $500), they may have good reason to file a motion to suppress. Defense counsel should be vigilant for the possible use of this surveillance to build prosecutions of their clients and consider challenging this potentially illegal and unconstitutional bulk surveillance.

III. Potential Challenges

Defense attorneys should note whether their client was involved in any money transfer since 2010 that exceeded $500, particularly if it involved a southwest-border state, Mexico, or was between any U.S. state and one of the 23 countries and territories mentioned above.[25] If your client's activity fell within the scope of this bulk surveillance program, even if the wire transfer is not central to the prosecution's case, this information could be useful to challenge the evidence or leverage a more favorable outcome.

A. Fourth Amendment

There are at least three Fourth Amendment arguments that defense counsel may advance in challenging evidence derived from this bulk wire transfer surveillance: (1) the summonses' or subpoenas' overbreadth and lack of relevance to any particular investigation make them unreasonable; (2) there is a reasonable expectation of privacy in these records, making their bulk acquisition a Fourth Amendment search (notwithstanding the government's near-certain invocation of the third-party doctrine); and (3) government access to these records intrudes on people's proprietary interest in the records, constituting a Fourth Amendment search under the property-based (i.e., trespass) doctrine.

1. *Lack of relevance to an identified criminal investigation*

The Fourth Amendment imposes a reasonableness requirement on subpoenas, including the administrative subpoenas and summonses at issue here. And there is no shortage of Fourth Amendment case law from the Supreme Court or circuit courts explaining that administrative subpoenas may only seek information that is relevant and material to the investigation that law

[23] Letter from Sen. Wyden, *supra* note 2.
[24] *See* FED. DEPOSIT INS. CORP., HOW AMERICA BANKS: HOUSEHOLD USE OF BANKING AND FINANCIAL SERVICES 1-2, 36 (2019), https://www.fdic.gov/analysis/household-survey/2019report.pdf.
[25] *See supra* note 2.

enforcement agents are conducting.[26] Such subpoenas may not be grossly overbroad,[27] nor grossly overburdensome.[28]

Here, defense counsel should argue the bulk summonses and subpoenas used to populate TRAC's database cannot possibly pass muster under this reasonableness test: A summons seeking six months' or a year's worth of records of all wire transfers that exceeded $500 and were sent to or from one or more states does not seek information "relevant" to an ongoing investigation.[29] Moreover, the prospective nature of the requests means that they were very likely not relevant to an existing investigation at the time they were issued. These summonses are unconstitutional. And because they could not constitutionally authorize the sweeping collection of data by HSI, the Arizona AG, and TRAC, everything derived from them should be suppressed.

To this relevancy argument, the prosecution might raise a standing counterargument: Can the accused challenge the summonses without demonstrating a reasonable expectation of privacy or a property interest in the records? Or is it only the recipient of the subpoena (i.e., the wire transfer company) that has standing to challenge it on relevancy grounds? Defense counsel should be prepared (hopefully by successfully using the discovery suggestions below) to respond by showing that the accused has a sufficient interest in their own records that were returned by the subpoena to maintain a Fourth Amendment challenge. Counsel may also argue that an overbroad and unreasonable subpoena is invalid from its inception, amounting to a request supported by no legal process at all.[30]

---

[26] *See, e.g.*, McLane Co., Inc. v. Equal Emp't Opportunity Comm'n, 137 S. Ct. 1159, 1165 (2017) ("[A] district court should 'satisfy itself that the charge is valid and that the material requested is "relevant" to the charge.'") (quoting Univ. of Pa. v. Equal Emp't Opportunity Comm'n, 493 U.S. 182, 191 (1990)); United States v. Powell, 379 U.S. 48, 57-58 (1964) ("[The Commissioner] must show that the . . . inquiry may be relevant to the purpose . . . ."); Presley v. United States, 895 F.3d 1284, 1288-89 (11th Cir. 2018) (holding an administrative agency must demonstrate an investigation's "legitimate purpose" and that "the information summoned is relevant to that purpose . . . ."); *see also* WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 4.13(a), (c) (6th ed. 2021) ("The second standard of reasonableness suggested in [*Okla. Press Publ'g Co. v.*] *Walling*[, 327 U.S. 186 (1946),] is the requirement that the subpoenaed documents be relevant to the investigatory body's inquiry.").

[27] *See* Equal Emp't Opportunity Comm'n, v. Royal Caribbean Cruises, Ltd., 771 F.3d 757, 762 (11th Cir. 2014) (holding an EEOC administrative subpoena was overbroad in seeking information "at best tangentially relevant" to the plaintiff's discrimination charge); *see also* State *ex rel.* Goddard v. W. Union Fin. Servs., Inc., 166 P.3d 916, 924 (Ariz. Ct. App. 2007) ("Subpoenas that are overbroad are not enforceable.").

[28] *See McLane Co., Inc.*, 137 S. Ct. at 1167 ("[T]he district court's decision whether to enforce a subpoena will turn either on whether the evidence sought is relevant to the specific charge before it or *whether the subpoena is unduly burdensome* in light of the circumstances.") (emphasis added).

[29] *See* Brief for Plaintiffs-Appellants at 1-2, ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015) (No. 14-42-CV) (alleging there was no way the government could demonstrate "reasonable grounds to believe that all Americans' call records" over 12 years were "'relevant' to an ongoing investigation").

[30] *Cf.* Groh v. Ramirez, 540 U.S. 551, 558 (2004) ("[T]he warrant was so obviously deficient that we must regard the search as 'warrantless' within the meaning of our case law."); United States v. Krueger, 809 F.3d 1109, 1123-24 (10th Cir. 2015) (Gorsuch, J., concurring) (stating a warrant issued outside of a magistrate's jurisdiction is "null and void").

2. *Reasonable expectation of privacy*

Counsel may also challenge the evidence by arguing that government collection of bulk records violates reasonable expectations of privacy, and the search is therefore unreasonable.[31] The financial records at issue here reveal personal details most people typically consider to be private. However, prosecutors are likely to invoke the third-party doctrine, arguing that *United States v. Miller*[32] and *Smith v. Maryland*[33] control because whoever wired the money revealed that transfer to a third party (e.g., Western Union). In *Miller*, the Supreme Court held that people have no reasonable expectation of privacy in information they voluntarily reveal to a bank, and thus the government can obtain account statements, canceled checks, and other similar records with a mere subpoena, rather than a warrant. Here, the prosecution will likely argue *Miller*'s holding forecloses any argument that there can be a reasonable expectation of privacy in similar financial records obtained from a wire transfer company. The defense should respond that *Miller* does not control the instant *bulk* surveillance because it is "qualitatively different"[34] from the limited set of canceled checks and bank statements pertaining to a single suspect at issue in *Miller*. In other words, whatever the third-party doctrine means in the context of a normal request for a particular suspect's records, it should not be extended to the sort of bulk surveillance occurring here. As the Supreme Court has explained, the simple "fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[35]

As the Supreme Court made clear in *Carpenter v. United States*, courts should not mechanically apply the third-party doctrine to new—and newly invasive—contexts.[36] Whatever might be revealed by a traditional request for a particular suspect's financial records, the dragnet search at issue here revealed an unprecedentedly comprehensive record of Americans' associations and activities—and not just for one person but for everyone who happened to use one of dozens of money transfer companies during the relevant time span.

---

[31] Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) ("When an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,' we have held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause.") (quoting Smith v. Maryland, 442 U.S. 735, 740 (1979)).

[32] 425 U.S. 435 (1976).

[33] 442 U.S. 735 (1979).

[34] *Carpenter*, 138 S. Ct. at 2216-17.

[35] *Id.* at 2217 (2018); *see also* Klayman v. Obama, 957 F. Supp. 2d 1, 32 (D.D.C. 2013) (holding the government's Bulk Telephony Metadata Program was "so different from a simple pen register" that applying *Smith* was "of little value in assessing whether" the bulk surveillance was a Fourth Amendment search).

[36] *Carpenter*, 138 S. Ct. at 2219 (2018) ("There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today. . . . In mechanically applying the third-party doctrine to this case, the Government fails to appreciate that there are no comparable limitations on the revealing nature of [cell site location information]."); *see also* Riley v. California, 573 U.S. 373, 393 (2014) ("A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom."); United States v. Knotts, 460 U.S. 276, 283-84 (1983) (permitting limited tracking of a particular suspect for a discrete period, but explaining that "dragnet type law enforcement practices" may require application of "different constitutional principles").

Additionally, defense counsel may argue that the government's *querying* of TRAC's database was a Fourth Amendment search, separate and apart from the search effected by the bulk subpoenas' acquisition of records. Courts have recognized that the obtaining of information and the querying or analysis of that information are separate Fourth Amendment events.[37] That is particularly true where records seized for one purpose are later searched for a completely separate purpose or in a separate investigation.[38] Here, law enforcement queries of TRAC's voluminous database of financial transactions are arguably a search; and because they were carried out with no legal process at all (i.e., no subpoena or warrant), they are unreasonable under the Fourth Amendment.

The success of this expectation-of-privacy argument turns, in part, on conveying to the court just how much can be learned from these records.[39] The more detail defense attorneys can show about the breadth of records collected pursuant to the subpoenas (not just as to their client, but as to the whole swath of people swept up in the bulk requests) and the wealth of information about people's associations and activities that can be inferred from those records, the greater chance of swaying the court that *Miller* does not control.

3. *Property-based search*

In *Carpenter*, Justice Gorsuch explained in a dissenting opinion that a person may retain Fourth Amendment rights in records within a third party's possession if that person retains at least some property-like interest in those records.[40] One source of such proprietary interests may be positive law. In *Carpenter*, Justice Gorsuch posited that the federal Telecommunications Act, 47 U.S.C. § 222, which restricts cell phone companies from selling or otherwise disclosing customers' location records without prior affirmative consent, may grant individuals enough of control over those location records to "rise to the level of a property right."[41]

---

[37] *See, e.g.*, United States v. Hasbajrami, 945 F.3d 641, 670 (2d Cir. 2019) ("[Q]uerying that stored data does have important Fourth Amendment implications, and those implications counsel in favor of considering querying a separate Fourth Amendment event that, in itself, must be reasonable."); Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 618 (1989) ("[T]he collection and subsequent analysis of . . . biological samples must be deemed [separate] Fourth Amendment searches . . . .").

[38] *See* People v. Hughes, 958 N.W.2d 98, 111 (Mich. 2020) ("The authority to seize an item does not necessarily eliminate one's expectation of privacy in that item and therefore allow the police to search that item without limitation.") (citing United States v. Jacobsen, 466 U.S. 109, 114 (1984)); *see also id.* at 113-14 ("[I]t is well established that a search warrant allows the state to examine property only to the extent authorized by the warrant.") (citing Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388, 394 n.7 (1971)); Brief of Amici Curiae ACLU et al. in Support of Defendant-Appellant at 33, State v. Burns, No. 20-1150 (Iowa Sup. Ct. Mar. 30, 2021), https://www.iowacourts.gov/courtcases/15314/briefs/5001/embedBrief ("[A]s a matter of administrative convenience, courts routinely permit police to seize entire hard drives pursuant to a warrant permitting search for only particular information, but require police to obtain a second warrant before searching for digital files outside the scope of the initial warrant.").

[39] *See* ACLU v. Clapper, 785 F.3d 787, 794 (2d Cir. 2015) ("That telephone metadata do not directly reveal the content of telephone calls . . . does not vitiate the privacy concerns arising out of the government's bulk collection of such data. . . . For example, a call to a single-purpose telephone number such as a 'hotline' might reveal that an individual is: a victim of domestic violence or rape; a veteran; suffering from an addiction of one type or another; contemplating suicide; or reporting a crime. Metadata can reveal civil, political, or religious affiliations; they can also reveal an individual's social status, or whether and when he or she is involved in intimate relationships.").

[40] *See Carpenter*, 138 S. Ct. at 2267-72 (Gorsuch, J., dissenting).

[41] *Id.* at 2272.

Here, the federal Gramm-Leach-Bliley Act requires financial institutions to protect the privacy of customers' financial records, and generally requires customer consent before such records may be disclosed.[42] State financial privacy statutes also restrict what financial institutions, including money transfer companies, can do with customers' financial records without those customers' consent.[43] These statutes mean that "customers have substantial legal interests in this information, including at least some right to include, exclude, and control its use,"[44] thus rendering the records *their* "papers" for Fourth Amendment purposes.[45] Notwithstanding how the third-party doctrine might interact with an argument asserting a reasonable expectation of privacy in these records, the implication of the property-based theory is that a government request for the records is a search or seizure to the same extent it would be if police sought a copy of the records directly from the accused's own files.

B. Statutory suppression

The HSI summonses and Arizona AG subpoenas almost certainly violated the statutes under which they were purportedly issued, 19 U.S.C. § 1509 and Ariz. Rev. Stat. § 13-2315.

Section 1509 confers on ICE limited authority in customs investigations to seek records "related to the importation of merchandise, including the assessment of customs duties."[46] But there is "no way these broad requests for bulk records would turn up only documents 'relevant' to specific investigations"[47] related to importation of merchandise.[48] HSI should have known as much, too, because the DHS Inspector General, in 2017, issued a report saying Customs and Border Patrol's Office of Professional Responsibility (CBP OPR) "misused the same authority" when it tried to unmask an anonymous Twitter user, concluding "CPB OPR 'may have exceeded the scope of its authority' and that it 'regularly' issued customs summonses in violation of agency policy."[49]

The Arizona AG was similarly on notice that its subpoenas were illegal under state law. In 2007, the Arizona Court of Appeals held that a bulk, prospective subpoena to Western Union violated Ariz. Rev. Stat. § 13-2315 because it was overbroad, and because it sought records of wire transfers that occurred wholly outside of Arizona and thus beyond the state's criminal

---

[42] 15 U.S.C. §§ 6801-6802.
[43] *See, e.g.*, California Financial Information Privacy Act, CAL. FIN. CODE § 4052.5 ("[A] financial institution shall not sell, share, transfer, or otherwise disclose nonpublic personal information . . . without the explicit prior consent of the consumer to whom the nonpublic personal information relates.") (2022) (effective July 1, 2004).
[44] *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting).
[45] *See* U.S. Const. amend. IV.
[46] Letter from Sen. Wyden, *supra* note 1.
[47] Matthew Guariglia, *Here's How ICE Illegally Obtained Bulk Financial Records from Western Union*, ELEC. FRONTIER FOUND. (Mar. 10, 2022), https://www.eff.org/deeplinks/2022/03/heres-how-ice-illegally-obtained-bulk-financial-records-western-union.
[48] An Arizona AG spokeswoman admitted as much, saying their office uses TRAC "to combat human and drug trafficking." Hackman & Volz, *supra* note 14.
[49] Letter from Sen. Wyden, *supra* note 1; *see also* JOHN ROTH, DEP'T OF HOMELAND SEC., OFF. OF INSPECTOR GEN., MANAGEMENT ALERT - CBP'S USE OF EXAMINATION AND SUMMONS AUTHORITY UNDER 19 U.S.C. § 1509, at 2-5 (2017), https://www.oig.dhs.gov/sites/default/files/assets/Mga/2017/oig-18-18-nov17.pdf.

jurisdiction under its anti-racketeering statute.[50] Therefore, much of the information requested was by definition not relevant to a permitted racketeering investigation.[51] Here, the subpoenas are even broader: while the 2007 subpoena sought records of money transfers involving *one* Mexican state (Sonora), the instant subpoenas sought records of transfers to or from *all* of Mexico or to/from any of the southwest-border states.

Section 1509 and section 13-2315 do not contain an express suppression remedy; but defense attorneys can seek an implied suppression remedy for the statutory violation, despite the uphill odds. Although the suppression remedy has been applied "primarily to deter constitutional violations,"[52] courts may suppress evidence for statutory violations where "the statutory violation implicates underlying constitutional rights."[53] For example, the Ninth Circuit has repeatedly suppressed evidence obtained in violation of a statute or procedural rule tied to constitutional interests.[54] Furthermore, courts "may use their supervisory power in some circumstances to exclude evidence taken from the defendant by 'willful disobedience of law.'"[55]

> "Despite a total lack of individualized suspicion, and based only on the happenstance of living in a southwestern state, details of a huge number of people's private financial transactions with family members and others were funneled straight to the government. Courts have made clear that narrow subpoena authorities like the one DHS relied on cannot be stretched to enable indiscriminate bulk collection of Americans' personal transactional data."
>
> — Nathan Freed Wessler
> Deputy Director, ACLU Speech, Privacy, & Technology Project[56]

IV. Discovery Requests

While not much is known about this bulk surveillance program, information obtained by the ACLU and Senator Wyden's office—about which money transfer companies have been subject

---

[50] State *ex rel.* Goddard v. W. Union Fin. Servs., Inc., 166 P.3d 916, 923-27 (Ariz. Ct. App. 2007).
[51] *Id.*
[52] Sanchez-Llamas v. Oregon, 548 U.S. 331, 348-49 (2006).
[53] United States v. Abdi, 463 F.3d 547, 556 (6th Cir. 2006); *see also* United States v. Dreyer, 804 F.3d 1266, 1278-79 (9th Cir. 2015) (en banc) (identifying specifically "the Fourth and Fifth Amendment concerns regarding unlawful searches"); Elkins v. United States, 364 U.S. 206, 223 (1960) ("[A] conviction resting on evidence secured through such a flagrant disregard of the procedure which Congress has commanded cannot be allowed to stand without making the courts themselves accomplices in willful disobedience of law.") (quoting McNabb v. United States, 318 U.S. 332, 345 (1943)).
[54] *See, e.g.*, United States v. Soto-Soto, 598 F.2d 545, 548 (9th Cir. 1979) (suppressing evidence obtained during border search that violated 19 U.S.C. § 482); United States v. Negrete-Gonzales, 966 F.2d 1277, 1283 (9th Cir. 1992) (suppressing evidence obtained in violation of Fed. R. Crim. P. 41).
[55] United States v. Payner, 447 U.S. 727, 735 n.7 (1980) (emphasis removed) (quoting *McNabb*, 318 U.S. at 345); *see also* United States v. Gatto, 763 F.2d 1040, 1046 (9th Cir. 1985).
[56] Hamed Aleaziz, *ICE Conducted Sweeping Surveillance of Money Transfers Sent to and from the US, a Senator Says*, BUZZFEED NEWS (Mar. 8, 2022), https://www.buzzfeednews.com/article/hamedaleaziz/ice-western-union-records-wyden.

to bulk summonses and subpoenas and which law enforcement agencies have access to TRAC[57]—provides a starting point for defense attorneys to assess whether evidence obtained or derived from TRAC may be at issue in their client's case. There is also reason to believe prosecutors have used parallel construction to conceal TRAC's role in investigating accused individuals.[58] Thus, defense counsel should be attentive to disclosure of *any* information about government acquisition of money transfer records in a case, even if it does not appear to involve TRAC.

Defense counsel should consider making the below discovery requests to glean more information about potential evidence being used against their clients:

☐ **Information pertaining to any money transfer**. Any and all state and/or federal records regarding your client that any law enforcement agency possesses, or at any time possessed, that were obtained or derived from any money transfer company or any platform or database containing records from a money transfer company. This request should include any and all communications between the wire transfer company and law enforcement that are related to such money transfers.

☐ **Information pertaining to TRAC**. Any and all state/federal records to do with your client that any law enforcement agency possesses, or at any time possessed, that were derived from TRAC's database(s). This request should include any and all communications between the money transfer company and law enforcement that are related to such wire transfers' being added to, removed from, or otherwise modified within TRAC's database(s), along with any and all communications between the money transfer companies, law enforcement agencies, and/or TRAC staff members or contractors acting on TRAC's behalf (e.g., communications between TRAC's tech support and law enforcement regarding a related wire transfer).

☐ **Searches, generally**. Similar to defense counsel in one of the few known prosecutions involving these bulk money transfer demands, request "[a]ll state or federal reports relating the circumstances of any search involving the defendant or [their] property . . . or any other search related to this case, listing the items seized and the information obtained as a result of these searches."[59]

☐ **Third parties' involvement**. Any and all communications between the money transfer company and the Arizona AG, HSI, and/or any other law enforcement agency that

---

[57] *See* E-mail from Richard Lebel, Exec. Dir., Transaction Record Analysis Ctr., to Carol Keppler (May 2, 2022, 2:17 PM), https://www.aclu.org/2022-05-02-trac-email-re-data-policy-mou-agency-list (providing list of law enforcement agencies and offices with access to TRAC); *see also* Letter from Sen. Wyden, *supra* note 2.

[58] In a federal prosecution in Montana, the government initially disclosed only a particularized subpoena issued to a money transfer company for the accused's records. Def.'s Br. in Supp. of Mot. to Suppress Evidence at 3, United States v. Escobedo, 2019 WL 6493943 (D. Mont. Dec. 3, 2019) (No. CR 19-113-BLG-SPW), ECF No. 22. Only later, in response to a motion to suppress, did the prosecutor reveal that earlier in the investigation, law enforcement had queried the TRAC database and obtained records about the accused. Response to Motion to Suppress Evidence at 3-4, *Escobedo*, 2019 WL 6493943, ECF No. 23.

[59] Request for Discovery at 2, United States v. Valdez-Paramo, No. 3:22-cr-00106-IM-3 (D. Or. filed Apr. 4, 2022), ECF No. 46.

concerned the bulk records of money transfers, including any summonses or other legal process issued to the money transfer company.

☐ **Law enforcement queries of TRAC's database**. All queries that law enforcement has run against the TRAC database, including the substance and volume of records that the agency received from TRAC in response to the agency's query or queries.

☐ **Number of individuals and records implicated**. Determine how many individuals were swept up in this bulk surveillance program, particularly in your jurisdiction; the total volume of records contained in TRAC's database; the total volume obtained from the money transfer company at issue in your case; and other information about the breadth and depth of records in TRAC's database(s).

V. Conclusion

This bulk money transfer surveillance program is yet another example of how law enforcement agencies attempt to circumvent Fourth Amendment protections against unreasonable searches and seizures. Rather than show probable cause to believe some likelihood that a crime involving a money transfer occurred, law enforcement has been prospectively issuing administrative subpoenas and summonses to money transfer companies, compelling them to surrender millions of customer records. Defense counsel whose clients' cases involve a wire transfer should seek to challenge this potentially unconstitutional evidence so that it is not used against their clients. Additionally, this will further place the government on notice that this sort of end run around the Constitution is unacceptable.