© Elnur | stock.adobe.com

Challenging the Warrantless Bulk Surveillance of Money Transfer Records

In March 2022, Sen. Ron Wyden revealed that law enforcement agencies in the United States have been secretly "operating an indiscriminate and bulk surveillance program that swept up millions of financial records about Americans."[1] These records have been accessible to law enforcement officers from hundreds of federal, state, and local agencies across the country, without any legal process or judicial oversight, and have been used to develop criminal prosecutions. Yet, the program operated in near-complete secrecy for years, and has been briefly addressed in just a single published court ruling on a motion to suppress — even though, based on what is currently known, there are significant arguments that it is unconstitutional.

This surveillance program, which began operating in 2010, is centered around a giant database established by the Arizona attorney general's office that contains records of virtually every money transfer of more than $500 sent to, from, or within the four southwest-border states (Arizona, California, New Mexico, and Texas) or Mexico, as well as transactions from anywhere in the United States to 23 foreign 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 Illinois to California, are tracked in the database, as are transactions between Nebraska and Spain, or Florida and Panama. The database now contains records of more than 150 million money transfers. Thousands of law enforcement officers from hundreds of agencies across the country have the ability to directly query the database without any subpoena or court order. And because of unequal access to traditional banking services, this surveillance program has a disproportionate effect on immigrants, people of color, and poor people, who often rely on money transfer services to send and receive funds.[3]

Like previously revealed bulk surveillance programs involving phone records and other data, this program — at a minimum — raises serious constitutional and legal concerns. Defense attorneys should be vigilant for the possible use of this surveillance data to build prosecutions of their clients, and ready to make legal arguments in support of a motion to suppress.[4]

Background

This story starts with an Arizona attorney general (AG) investigation into suspected illicit Western Union wire transfers from the United States to Mexico. In 2006, the Arizona AG's office issued a subpoena under a state anti-racketeering investigative statute, Ariz. Rev. Stat. § 13-2315, 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

BY NATHAN FREED WESSLER AND MAX BEHRMAN

three-year period."[5] Western Union resisted, and a state appellate court held the overbroad scope of the AG's subpoena was "not authorized by Arizona law" and amounted to a request for "limitless" investigative power.[6] The court quashed the subpoena, explaining that "[t]he Attorney General cites no case, and we have found none, in which an administrative request similar in scope to the one at issue has been upheld as reasonable."[7]

Unsatisfied, the Arizona AG proceeded to sue Western Union for violation of a state anti-money laundering statute. In 2010, the Arizona AG and Western Union reached a settlement to resolve that lawsuit.[8] The settlement required that Western Union, on an ongoing basis, provide the AG's office with information about every money transfer of more than $500 to or from Arizona, California, New Mexico, Texas, or Mexico.[9]

In 2014, shortly before the settlement was set to expire, Western Union and the Arizona AG entered into a second agreement that extended the bulk data production arrangement to 2019.[10] This second settlement also established a new 501(c)(3) nonprofit organization, the Transaction Record Analysis Center (TRAC), to "facilitate law enforcement access to the bulk data."[11] The agreement required Western Union to pay hundreds of thousands of dollars to fund TRAC's budget. Although TRAC is nominally an independent organization, under its bylaws its Board of Directors is chosen by the Arizona AG,[12] many of TRAC's officers are employees of the Arizona AG's office,[13] and its annual reports since at least 2018 list the organization's "known place of business" as the same physical address as the AG's office.[14] Indeed, the Department of Homeland Security (DHS) describes TRAC as "a database run by a state government."[15]

Once TRAC was up and running, Western Union began sending the money transfer records to TRAC instead of providing them to the Arizona AG. Moreover, although Western Union was the only company subject to an enforceable settlement agreement, "dozens of other money transfer businesses also provided TRAC with similar bulk transaction data";[16] 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."[17] Although initial reporting suggested that those companies had been providing records to TRAC "voluntarily," records disclosed in response to an ACLU public records request to the Arizona AG's office revealed that the AG has been sending prospective, annual bulk records subpoenas to a number of money transfer companies, directing each company to produce customer data on an ongoing basis over the next year.[18] The AG issued those subpoenas under Ariz. Rev. Stat. § 13-2315, the same anti-racketeering statute that a state appellate court held did not authorize the bulk money-transfer-records subpoena issued to Western Union in 2006.[19] The AG produced 140 of these subpoenas, issued between 2014 and 2021 to 18 money transfer companies, in response to the ACLU's public records request.[20]

By early 2023, TRAC's database had swollen to more than 150 million wire transfer records from Western Union and the other companies.[21]

TRAC's main purpose is to facilitate sharing of the money transfer records with other law enforcement agencies. On that count, it has succeeded: internal TRAC records state that as of early 2021, TRAC had provided access to the database to 12,000 individuals from 600 federal, state and local law enforcement agencies,[22] "who could mine the data for leads without being required to issue a warrant."[23] The ACLU has obtained and published TRAC's list of more than 700 law enforcement agencies and field offices that, as of May 2022, had current or previous access to the database.[24] Using direct log-ins supplied by TRAC, law enforcement agents can search for financial transactions of specific individuals, or analyze large numbers of transactions involving multiple people in specified geographic areas or worldwide.[25]

When the second settlement with Western Union expired in 2019, the company apparently took the position that it would not voluntarily continue providing records to TRAC. The Arizona AG sought assistance from DHS — via the Phoenix Field Office of Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) — "to compel [Western Union] to continue sharing data."[26] 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. HSI issued summonses every six months, which *prospectively* directed each company to turn over bulk money transfer data on an ongoing basis over the next six months. Separately, the San Juan field office of HSI was issuing summonses to at least two money transfer companies, Euronet and Viamericas, for bulk data on transfers from anywhere in the United States to 23 countries and territories, and to Maxi for records on transfers from 21 U.S. states to Colombia, the Dominican Republic, Venezuela, and the U.S. Virgin Islands.[27]

The HSI summonses were issued under the purported authority of 19 U.S.C. § 1509, an administrative subpoena statute conferring limited authority to request records related to importation of merchandise. As explained below, that statute clearly does not authorize HSI's indiscriminate summonses for these money transfer records.

This was not the first time that DHS had abused its customs summons authority. In March 2017, U.S. Customs and Border Protection (CBP) issued a summons under § 1509 to Twitter, seeking the identity of an anonymous Twitter user who had been posting tweets critical of federal immigration agencies. After Twitter sued to quash the summons on First Amendment and statutory grounds, CBP withdrew it. A subsequent report by the DHS Inspector General (IG) recognized that § 1509 "addresses ascertainment, collection, and recovery of *customs duties*," yet "CBP's purpose in issuing the summons to Twitter was unrelated to the importation of merchandise or the assessment and collection of customs duties."[28] Therefore, "CBP may have exceeded the scope of its authority under Section 1509 when it issued the summons to Twitter."[29] The IG found that CBP investigators had issued § 1509 summonses dozens of times in investigations having nothing to do with importation of merchandise, including drug investigations, and even internal investigations into CBP employees suspected of violating the agency's sick leave policy.[30] In response to the IG's findings, CBP agreed to update its policy and trainings to end abusive uses of § 1509.[31]

The DHS IG report apparently had little effect on ICE's practices, however. Far from seeking particular evidence relevant to the investigation of offenses related to importation of merchandise,

the HSI summonses at issue here requested bulk records of money transfers, including transfers that occurred wholly within the United States. And instead of identifying and requesting *existing* records, as would be typical of a subpoena, the summonses *prospectively* directed the companies to transmit records on an ongoing basis.[32]

After learning about this program in 2021, Sen. Wyden contacted HSI to request a briefing. In response, HSI "immediately terminated" its summonses under the customs statute.[33] 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, Sen. Wyden sent a letter to the DHS IG, requesting an investigation of this "indiscriminate and bulk surveillance program."[34] And in January 2023, after learning that the DEA and FBI were also sending subpoenas to money transfer companies and compelling them to send bulk records to TRAC, Sen. Wyden wrote to the Department of Justice Inspector General, seeking an investigation of violations of law or policy by agencies within DOJ.[35]

The bulk wire transfer surveillance program is another troubling example of law enforcement attempting to circumvent Fourth Amendment protections against unreasonable searches and seizures.

The public still lacks many details about this program. Reporting by the *Wall Street Journal* has identified one federal narcotics prosecution in the District of Oregon where the wire transfer records were used,[36] and a federal court decision from Montana denying a motion to suppress provides details about another case,[37] but the breadth of use in other state and federal cases is as yet unknown. And although the Arizona AG has released copies of its bulk subpoenas, HSI, the FBI, and the DEA have yet to make public copies of the summonses or subpoenas they served on money transfer companies. The ACLU submitted a Freedom of Information Act request to HSI in March 2022 but has yet to receive documents.[38]

Legal Arguments

If evidence obtained or derived from queries of the TRAC database may be at issue in a client's case, arguments are available to seek suppression. If counsel's client sent or received money transfers that may have contributed to the government's investigation, the client may have good reason to file a motion to suppress. This article discusses the legal arguments supporting suppression and concludes with tips for seeking discovery to shed light on the government's conduct.

Fourth Amendment

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

1. Lack of Relevance to an Identified Criminal Investigation and Overbreadth

The Fourth Amendment imposes a reasonableness requirement on subpoenas, including the administrative subpoenas and summonses at issue here. Such process may only seek information that is (1) relevant and material to an ongoing investigation,[39] (2) not grossly overbroad,[40] and (3) not overly burdensome for the recipient to comply with.[41] The bulk summonses and subpoenas used to populate the enormous TRAC database cannot possibly pass muster under this reasonableness test.

"[D]ocument subpoenas typically seek the records of a particular individual or corporation under investigation, and cover particular time periods when the events under investigation occurred."[42] The U.S. Court of Appeals for the Eighth Circuit has applied this rule in the context of a subpoena to Western Union for customer records, finding that a subpoena for a subset of records from a single Western Union office over "a relatively short period of time" was reasonable but that a more "sweeping" request might well be unreasonable under the Fourth Amendment.[43] A subpoena 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. Indeed, the entire point of the subpoenas appears to have been to gather records *in anticipation* of their possibly being relevant to some unspecified and unknown future investigations. They amount to a "claim of 'an unlimited right of access to the … records, relevant or irrelevant, in the hope that something will turn up.'"[44]

As the Second Circuit explained when rejecting a government program involving prospective bulk requests for telephone dialing records, subpoenas for "records that do not *yet* exist" are invalid because they indiscriminately seek records not yet created, whose relevance cannot be known at the time they are requested.[45] For that reason, such prospective data-gathering subpoenas are virtually unheard of: as the Second Circuit observed, the government in that case could not identify any other "subpoena that is remotely comparable to the real-time data collection undertaken under this program."[46]

Further, even if the subpoenas did identify some existing investigation as to which certain financial records were purportedly relevant, the scope of these requests would undoubtedly be overbroad in relation to such an investigation. Like the government's discredited — and now-defunct — bulk telephone metadata surveillance program, the indiscriminate collection of money transfer records means "[t]he records demanded are not those of suspects under investigation."[47] Such subpoenas require money transfer companies to "turn over records on an 'ongoing … basis' — with no foreseeable end point, no requirement of relevance to any *particular set of facts*, and no limitations as to subject matter or individuals covered,"[48] other than the greater-than-$500 and geographic limits. The subpoenas are invalid because the gov-

ernment cannot indiscriminately collect bulk surveillance data without first making "a showing of relevance to a particular authorized investigation *before* collecting the records."[49]

Because they lack relevance and are overbroad, the bulk summonses and subpoenas are unreasonable under the Fourth Amendment, and defense counsel should seek suppression of any records obtained or derived from them.[50]

The prosecution may contest the accused's entitlement to seek suppression, on the ground that only the recipient of the subpoena (i.e., the wire transfer company) has standing to challenge a summons on relevancy grounds, since wire transfer customers lack a reasonable expectation of privacy in the records. This precise question has not often been litigated, but courts have permitted accused individuals to challenge demands for records held by third parties when the information relates to their activities and they are raising constitutional and statutory challenges.[51] Indeed, as described below, defense counsel can argue that people do have a privacy interest in these records sufficient to confer standing under the Fourth Amendment. Finally, counsel may argue that an overbroad and unreasonable subpoena is invalid from its inception and so is akin to a request supported by no legal process at all.[52]

2. Reasonable Expectation of Privacy

Counsel may also challenge the evidence on the basis that government collection of bulk records violates reasonable expectations of privacy, and the search is therefore unreasonable.[53]

The financial records at issue here reveal personal details most people typically consider to be private. However, prosecutors are likely to invoke the so-called "third-party doctrine," arguing that *United States v. Miller*[54] controls because the individual who wired the money revealed that transfer to a third party, the money transfer company. 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 contend that *Miller*'s holding forecloses any argument that there can be a reasonable expectation of privacy in similar financial records obtained from a money transfer company. At least one court has accepted this argument in the context of TRAC records, holding that the accused "lost any expectation of privacy he had in the [money transfer] information when he turned it over to the third parties" — i.e., the money transfer companies — in the course of wiring funds.[55]

The defense should respond that whatever *Miller* means for traditional subpoenas for a specific suspect's records, it does not control a bulk request for *everyone's* records. Such dragnet surveillance is "qualitatively different"[56] 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."[57]

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.[58] 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 people's associations and activities — and not just for one person but for large numbers of people who happened to use one of dozens of money transfer companies during the relevant time span. As the Supreme Court has recognized, even where limited tracking of a particular suspect for a discrete period is permissible, "dragnet type law enforcement practices" may require application of "different constitutional principles."[59]

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 acquisition of records using the bulk subpoenas. Courts have recognized that the obtaining of information and the querying or analysis of that information are separate Fourth Amendment events.[60] That is particularly true where records seized for one purpose are later searched for a completely separate purpose or in a separate investigation.[61]

The success of the expectation-of-privacy argument may turn, in part, on conveying to the court just how much can be learned from these records.[62] 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 conveying to the court why *Miller* does not control.[63]

3. Property-based Search

Independent of the reasonable-expectation-of-privacy test, counsel should also argue that access to these financial records is a search under the property-based theory of the Fourth Amendment.[64]

In *Carpenter*, Justice Gorsuch explained in a dissenting opinion that a person may retain Fourth Amendment rights in digital records within a third party's possession if that person can claim a property-like interest in those records.[65] One source of such proprietary interests may be positive law — statutes and common law doctrines conferring rights on individuals. In

Justice Gorsuch's view, if sources of positive law grant "substantial legal interests [to] this information, including at least some right to include, exclude, and control its use,"[66] there may be a sufficient property interest to trigger Fourth Amendment protection. Justice Gorsuch posited that the federal Telecommunications Act, 47 U.S.C. § 222, which restricts cellphone companies from selling or otherwise disclosing customers' location records without the customers' consent, may grant individuals enough of control over those location records to "rise to the level of a property right."[67] Thus, warrantless government requests for those records may interfere with a person's property and constitute a Fourth Amendment search.

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.[68] State financial privacy statutes also restrict what financial institutions, including money transfer companies, can do with customers' financial records without those customers' consent.[69] These statutes mean that "customers have substantial legal interests in this information, including at least some right to include, exclude, and control its use,"[70] thus rendering the records *their* "papers" for Fourth Amendment purposes.[71] 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.

Statutory Violation

The HSI summonses and the Arizona AG subpoenas 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."[72] But there is "no way these broad requests for bulk records would turn up only documents 'relevant' to specific investigations"[73] related to importation of merchandise.[74] HSI should have known as much because the DHS Inspector General, in 2017, issued a report saying CBP's Office of Professional Responsibility (CBP OPR) "misused the same authority" when it demanded records that would unmask an anonymous Twitter user, concluding that "CPB OPR 'may have exceeded the scope of its authority' and that it 'regularly' issued customs summonses in violation of agency policy."[75]

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 jurisdiction under its anti-racketeering statute.[76] Therefore, much of the information requested was by definition not relevant to a permitted racketeering investigation.[77] The subpoenas at issue here are even broader: while the 2007 subpoena sought records of money transfers involving one Mexican state (Sonora), the recent subpoenas seek 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 express suppression remedies, but defense attorneys may argue for an implied suppression remedy for the statutory violation. Although the suppression remedy has been applied "primarily to deter constitutional violations,"[78] courts may suppress evidence for statutory violations where "the statutory violation implicates underlying constitutional rights."[79] For example, the Ninth Circuit has repeatedly suppressed evidence obtained in violation of a statute or procedural rule tied to constitutional interests.[80] Furthermore, courts "may use their supervisory power in some circumstances to exclude evidence taken from the defendant by 'willful disobedience of law.'"[81]

Make Smart Use of Discovery Requests

Information obtained by the ACLU and Sen. Wyden's office about which money transfer companies have been subject to bulk summonses and subpoenas, and about which law enforcement agencies have access to TRAC,[82] 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. But more information will be needed to bring a motion to suppress.

There is reason to believe prosecutors have used parallel construction to conceal TRAC's role in investigating accused individuals. 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. In a federal prosecution in Montana, the government initially disclosed only a particularized subpoena issued to a money transfer company for the defendant's records.[83] 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.[84]

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

- **Information pertaining to any money transfer.** Request any and all state and/or federal records regarding the 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 should include any and all communications between the money transfer company and law enforcement related to the money transfers to or from counsel's client.

- **Information pertaining to TRAC.** Request any and all state and/or federal records regarding the 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 the wire transfers' being added to, removed from, or otherwise modified within TRAC's database(s), such as 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 relevant wire transfer).

- **Law enforcement queries of TRAC's database**. Request records relating to all queries that law enforcement has submitted to TRAC, including the substance and volume of records that law enforcement received in response from TRAC regarding the query or queries.

- **Third parties' involvement**. Request any and all communications between the money transfer company and the Arizona attorney general, HSI, and/or any other law enforcement agency that concerned the bulk records of wire transfers, including any summonses or other legal process issued to the money transfer company.

- **Number of individuals and records implicated**. Request records reflecting how many individuals were swept up in this bulk surveillance program, particularly in defense counsel's jurisdiction, the total volume of records contained in TRAC's database, the total volume obtained from the money transfer company at issue in the client's case, and other information about the breadth and depth of the records in TRAC's database.

- **Searches, generally**. Like 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."[85]

Conclusion

This bulk wire transfer surveillance program is yet another troubling example of law enforcement attempting to circumvent Fourth Amendment protections against unreasonable searches and seizures. Rather than investigate an already committed crime and attempt to determine whether probable cause exists to obtain a search warrant for a suspect's money transfer records, law enforcement has been issuing administrative subpoenas to wire transfer companies, *prospectively* compelling them to surrender millions of customer records.

To adequately defend their clients, defense attorneys whose clients' cases involve or may involve a wire transfer should seek discovery and suppression of this potentially unconstitutional evidence. Doing so may not only benefit the client but could ultimately shed light on this indiscriminate bulk surveillance program, which disproportionately affects individuals from vulnerable communities who rely more heavily on money transfer services.

The authors thank Ashley Gorski, Brett Max Kaufman, Noam Shemtov, and Patrick Toomey for their feedback, suggestions, and assistance with this article.

Notes

1. Letter from U.S. Sen. 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. *See* Letter from U.S. Sen. 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. 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. *Id.*

3. *See generally* 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.

4. *See generally* NACDL, Practice Advisory: Law Enforcement Access to Wire Transfer Data (2022), https://www.nacdl.org/Document/Practice-Advisory-Law-Enforcement-Access-to-Wire-T.

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

6. *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").

7. *Id.* at 924.

8. 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.

9. *Id.* at 6, 11.

10. 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.

11. Letter from Sen. Wyden, *supra* note 1.

12. Transaction Record Analysis Ctr., Amendment to By-Laws of the Transaction Record Analysis Center, Inc. 2 (2017), https://www.aclu.org/foia-document/2017-04-10-amendment-laws-trac-incpdf.

13. For instance, in 2022, TRAC's Director was also the state AG's Director of External Affairs. *See About the Office of Attorney General*, *Organizational Chart*, Ariz. Att'y Gen., https://www.azag.gov/sites/default/files/docs/office/AZAGO_Org_Chart_Eff_07-2021.pdf (last visited Aug. 9, 2022). Additionally, the addresses for three TRAC officers, as listed on the website for the Arizona Corporation Commission, are the same address as the state AG's office. *See Entity Information*, Ariz. Corp. Comm'n, https://ecorp.azcc.gov/BusinessSearch/BusinessInfo?entityNumber=20200818 (last visited Aug. 9, 2022).

14. *See, e.g.*, *2022 Annual Report*, Ariz. Corp. Comm'n (July 8, 2022), https://ecorp.azcc.gov/CommonHelper/GetFilingDocuments?barcode=22070808386870; *2018 Annual Report*, Ariz. Corp. Comm'n (July 10, 2018), https://ecorp.azcc.gov/CommonHelper/GetFilingDocuments?barcode=18071013303491.

15. U.S. Dep't of Homeland Sec., Privacy Impact Assessment for the Repository for Analytics in a Virtualized Environment (RAVEn) 25 (2020), https://www.dhs.gov/sites/default/files/2022-06/privacy-pia-ice055-raven appendixbupdate-june2022_1.pdf.

16. Letter from Sen. Wyden, *supra* note 1.

17. 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) [hereinafter TRAC 2021 Board Meeting Minutes], https://www.aclu.org/2021-1-15-minutes-board-meeting.

18. *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.

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

20. *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).

21. 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-program-captures-money-transfers-between-u-s-and-more-than-20-countries-11674019904. The volume of other companies' voluntary 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.

22. Walter-Johnson & Wessler, *supra* note 18; TRAC 2021 Board Meeting Minutes, *supra* note 17.

23. Hackman & Volz, *supra* note 21.

24. *See* Email 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.

25. Raytheon|Websense, Arizona Financial Crimes Task Force 2 (2015) (on file with authors); *see also* Forcepoint, Arizona Financial Crimes Task Force 2 (2017), https://www.forcepoint.com/sites/default/files/case_study_downloads/casestudy_arizona_financial_crimes_task_force_en.pdf [https://web.archive.org/web/20220310171939/https:/www.forcepoint.com/sites/default/files/case_study_downloads/casestudy_arizona_financial_crimes_task_force_en.pdf].

26. Hackman & Volz, *supra* note 21; *see also* Letter from Sen. Wyden, *supra* note 1.

27. Letter from Sen. Wyden, *supra* note 2.

28. 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 2–3 (2017), https://www.oig.dhs.gov/sites/default/files/assets/Mga/2017/oig-18-18-nov17.pdf.

29. *Id.* at 3.

30. *Id.* at 4.

31. *Id.* at 6–8.

32. Letter from Sen. Wyden, *supra* note 1 (emphasis added).

33. *Id.*

34. *Id.*

35. Letter from Sen. Wyden, *supra* note 2.

36. Hackman & Volz, *supra* note 21; *see also* United States v. Munoz et al., No. 3:22-cr-00106-IM (D. Or.).

37. United States v. Escobedo, No. CR 19-113-BLG-SPW, 2019 WL 6493943 (D. Mont. Dec. 3, 2019).

38. Freedom of Information Request from ACLU to U.S. Immigr. & Customs Enf't (Mar. 9, 2022), https://www.aclu.org/foia-request-hsi-phoenix-field-office-regarding-bulk-collection-wire-transfer-records; Public Records Request from ACLU to Office of the Ariz. Att'y Gen. (Mar. 10, 2022), https://www.aclu.org/public-records-request-az-attorney-general-concerning-bulk-collection-wire-transfer-records.

39. *See, e.g.*, McLane Co., Inc. v. Equal Emp. Opportunity Comm'n, 581 U.S. 72, 76 (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. 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.").

40. *See* Equal Emp. 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.").

41. *See McLane Co., Inc.*, 581 U.S. at 81 ("[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).

42. ACLU v. Clapper, 785 F.3d 787, 813 (2d Cir. 2015).

43. In re Grand Jury Proceedings: Subpoenas Duces Tecum, 827 F.2d 301, 304 (8th Cir. 1987).

44. *Okla. Press Publ'g Co.*, 327 U.S. at 207 n.40 (quoting Fed. Trade Comm'n v. Am. Tobacco Co., 264 U.S. 298, 305–06 (1924)).

45. *Clapper*, 785 F.3d at 813.

46. *Id.*

47. *Id.*

48. *Id.* at 814 (emphasis added).

49. United States v. Moalin, 973 F.3d 977, 996 (9th Cir. 2020).

50. *Cf.* Carpenter v. United States, 138 S. Ct. 2206, 2221–22 (2018) ("[T]his Court has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy. . . . If the choice to proceed by subpoena provided a categorical limitation on Fourth Amendment protection, no type of record would ever be protected by the warrant requirement.").

51. *See Moalin*, 973 F.3d at 993–94 (challenging bulk collection of call records held by third party); *cf. Clapper*, 785 F.3d at 801 ("Whether or not such claims prevail on the merits, appellants surely have standing to allege injury from the collection, and maintenance in a government database, of records relating to them."); Amidax Trading Grp. v. S.W.I.F.T. SCRL, 671 F.3d 140, 147 (2d Cir. 2011) ("To establish an injury in fact—and thus, a personal stake in this litigation—[Amidax] need only establish that its information was obtained by the government.").

52. *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").

53. *Carpenter*, 138 S. Ct. at 2213 ("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.") (cleaned up).

54. 425 U.S. 435 (1976); *see also* Smith v. Maryland, 442 U.S. 735 (1979).

55. United States v. Escobedo, No. CR 19-113-BLG-SPW, 2019 WL 6493943, at *2 (D. Mont. Dec. 3, 2019).

56. *Carpenter*, 138 S. Ct. at 2216–17.

57. *Id.* at 2217; *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).

58. *Carpenter*, 138 S. Ct. at 2219 ("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.").

59. United States v. Knotts, 460 U.S. 276, 283–84 (1983).

60. *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 . . . .").

61. *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)); 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/embed Brief ("[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.").

62. *See, e.g.*, 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.").

63. *Cf. Carpenter*, 138 S. Ct. at 2218 ("Critically, because location information is continually logged for all of the 400 million devices in the United States —not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone.").

64. *See* United States v. Jones, 565 U.S. 400, 409 (2012) ("[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.").

65. *See Carpenter*, 138 S. Ct. at 2267–72 (Gorsuch, J., dissenting).

66. *Id.* at 2272.

67. *Id.*

68. 15 U.S.C. §§ 6801–6802.

69. *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.").

70. *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting).

71. *See* U.S. CONST. AMEND. IV.

72. Letter from Sen. Wyden, *supra* note 1.

73. 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.

74. An Arizona AG spokesperson admitted as much, saying their office uses TRAC "to combat human and drug trafficking." Hackman & Volz, *supra* note 21.

75. Letter from Sen. Wyden, *supra* note 1; *see also* JOHN ROTH, *supra* note 28, at 2–5.

76. State *ex rel.* Goddard v. W. Union Fin. Servs., Inc., 166 P.3d 916, 923–27 (Ariz. Ct. App. 2007).

77. *Id.*

78. Sanchez-Llamas v. Oregon, 548 U.S. 331, 348–49 (2006).

79. 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)).

80. *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).

81. 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).

82. *See* Email from Richard Lebel, *supra* note 24 (providing list of law enforcement agencies and offices with access to TRAC); *see also* Letter from Sen. Wyden, *supra* note 2.

83. 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.

84. Response to Motion to Suppress Evidence at 3–4, *Escobedo*, 2019 WL 6493943, ECF No. 23.

85. 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.

About the Authors

Nathan Freed Wessler is the Deputy Director of the ACLU Speech, Privacy, and Technology Project.

Nathan Freed Wessler
American Civil Liberties Union Foundation
New York, New York
212-549-2550
EMAIL nwessler@aclu.org.

Max Behrman is the Legal Fellow at the NACDL Fourth Amendment Center.

Max Behrman
NACDL
Washington, DC
202-331-4971
EMAIL mbehrman@nacdl.org