

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

UNITED STATES OF AMERICA,)
)
 v.)
)
CHARLES EDWARD LITTLEJOHN,)
)
 Defendant.)
_____)

Criminal Number: 1:23-cr-343

GOVERNMENT’S SENTENCING MEMORANDUM

Defendant Charles Edward Littlejohn is scheduled to be sentenced on January 29, 2024, at 10 a.m. The United States respectfully submits this memorandum in connection with sentencing.

PRELIMINARY STATEMENT

Over the course of more than two years, Defendant—a consultant at the U.S. Department of the Treasury’s Internal Revenue Service (“IRS”)—abused his position by unlawfully disclosing thousands of Americans’ federal tax returns and other private financial information to multiple news organizations. After applying to work as an IRS consultant with the intention of accessing and disclosing tax returns, Defendant weaponized his access to unmasked taxpayer data to further his own personal, political agenda, believing that he was above the law. A free press and public engagement with the media are critical to any healthy democracy, but stealing and leaking private, personal tax information strips individuals of the legal protection of their most sensitive data. Everyone is entitled to equal protection under the law. And Defendant’s betrayal of the public trust merits significant punishment. For the reasons that follow, the Court should sentence Defendant to the statutory maximum of 60 months’ imprisonment.

BACKGROUND

I. The Defendant and His Offense¹

Between 2008 and 2013, Defendant worked intermittently for Company A—a consulting firm that services public and private clients—principally on contracts the company had obtained with the IRS. *See* ECF No. 9 (Plea Agreement Factual Basis) (“Factual Basis”) at ¶¶ 1-2. During much of this time, he was authorized, pursuant to 26 U.S.C. § 6103(n), to access vast amounts of unmasked taxpayer data, including tax returns and return information, on IRS databases. *Id.* at ¶ 3. He received regular trainings on protecting taxpayer data and about the criminal consequences of inspecting or disclosing, without authorization, tax returns and return information. *See* ECF No. 16 (Draft Presentence Investigation Report) (“PSR”) at ¶ 13.

A. Defendant’s Disclosure of Public Official A’s Tax Returns and Return Information

In 2017, Defendant once again sought work with Company A, with the hope and expectation of accessing and disclosing tax returns and return information associated with Public Official A, a high-ranking government official. Factual Basis at ¶ 5; PSR at ¶ 16. Defendant viewed Public Official A as “dangerous and a threat to democracy,” and he intended to obtain Public Official A’s taxpayer information from the IRS and provide it to the public. PSR at ¶ 16. In or about September 2017, Company A in fact re-hired Defendant and—in February 2018—granted him access to unmasked taxpayer data. PSR at ¶ 16.

¹ Defendant pled guilty to making unauthorized disclosures of tax information in violation of 26 U.S.C. § 7213(a)(1). This five-year felony is the most serious offense for leaking tax information. While the applicable guideline range here is the highest possible in light of the facts, as explained in detail later in this memorandum, that range is flatly inconsistent with the gravity of the offense. An upward departure and/or upward variance to the statutory maximum of 60 months’ imprisonment is warranted based on the uniquely egregious conduct here.

By late 2018, Defendant had developed a sophisticated, detailed plan to secretly download Public Official A’s tax returns and return information from a particular internal IRS database on which he learned it was stored (the “Database”). Factual Basis at ¶ 5; PSR at ¶¶ 16-17. Rather than directly search the Database for Public Official A’s taxpayer data—which might have triggered scrutiny or detection of his scheme—Defendant queried the database using more generalized parameters that would nevertheless collect Public Official A’s tax return and return information (as well as return and return information for related entities and individuals) in the resulting data set. Factual Basis at ¶ 5; PSR at ¶ 17.

The next problem Defendant faced was actually extracting the data associated with Public Official A from the Database. Defendant learned that IRS protocols could detect and prevent large downloads or uploads from IRS systems and devices. Factual Basis at ¶ 6; PSR at ¶¶ 17-18. But on or about November 30, 2018, he exploited a loophole in those controls by uploading the stolen tax return and return information to a private website that he controlled. Factual Basis at ¶ 6; PSR at ¶¶ 17-18. He thereafter used a personal computer to download the data from that private website. Factual Basis at ¶ 6; PSR at ¶¶ 17-18. From the original data set stored on his personal computer, Defendant made copies and stored them on personal data storage devices such as his Apple iPod (which, using his specialized technical skills, he had configured as a personal hard drive). Factual Basis at ¶ 6; PSR at ¶ 18.

Approximately six months later, in or about May 2019, Defendant contacted a news organization (“News Organization 1”) to discuss potentially providing the organization with a copy of Public Official A’s tax records. Factual Basis at ¶ 7; PSR at ¶ 19.

Subsequently, between August and October 2019, Defendant disclosed Public Official A’s tax records to News Organization 1. Factual Basis at ¶ 7; PSR at ¶ 19. Defendant then stole

additional tax returns and return information associated with Public Official A (along with related individuals and entities) and provided those to News Organization 1 as well. Factual Basis at ¶ 8; PSR at ¶ 20. On or about September 27, 2020, News Organization 1 published the first of several articles that publicly disclosed information contained in Public Official A's tax returns. Factual Basis at ¶ 9; PSR at ¶ 21.

B. Defendant's Disclosure of Thousands of Other Returns and Return Information

But leaking Public Official A's tax returns and return information did not satisfy Defendant's appetite for disclosing taxpayer data. In or about July and August 2020, Defendant accessed unmasked IRS data associated with thousands of the nation's wealthiest people, including returns and return information dating back over 15 years. Factual Basis at ¶ 10; PSR at ¶ 22. Replicating his earlier mechanism for extracting material from the Database, Defendant downloaded the relevant data and uploaded it to a private website. Factual Basis at ¶ 11; PSR at ¶ 22. In uploading the taxpayer returns and return information to a private website, Defendant used two virtual machines (essentially simulated versions of physical computers). *Id.* In order to conceal his activities, Defendant promptly destroyed these machines after he used them to steal the data from IRS. *Id.*

In or about September 2020, Defendant contacted a second news organization ("News Organization 2") and provided a reporter with a copy of the data on the nation's wealthiest taxpayers that he had stolen from the IRS. Factual Basis at ¶ 12; PSR at ¶ 23. Defendant provided the data by mailing it to News Organization 2 on a password-protected personal data storage device. *Id.* In November 2020, Defendant provided the device's password to a journalist at News Organization 2. *Id.* Beginning in or about June 2021, News Organization 2 published the first in a

series of nearly 50 articles using the return and return information Defendant had disclosed. *See* Factual Basis at ¶ 13; PSR at ¶ 23.

C. Defendant’s Efforts to Obstruct the Investigation

Throughout Defendant’s scheme, he undertook efforts to obstruct and impede the investigation that he anticipated would follow the publication of the tax data he had stolen. For example, in 2021—before returning his assigned IRS laptop when he ceased working on Company A’s IRS contract—Defendant deleted nearly all the files in his user profile. Factual Basis at ¶ 14(a); PSR at ¶ 24(a). Additionally, as described above, he destroyed the virtual machines he had used to facilitate his theft of taxpayer returns and return information from the Database. Factual Basis at ¶ 14(b); PSR at ¶ 24(b). Finally, after uploading returns and return information to the private website, Defendant promptly contacted the domain registration service to cancel the private website’s domain registration. Factual Basis at ¶ 14(c); PSR at ¶ 24(c).

II. The Plea Agreement and the Presentence Report

On September 29, 2023, the United States charged Defendant pursuant to an Information with violating 26 U.S.C. § 7213(a)(1), which imposes criminal liability on IRS contractors and employees who “willfully [] disclose to any person, except as authorized in this title, any return or

return information.”² ECF No. 1 (Information). On October 12, 2023, Defendant pled guilty to the Information, ECF No. 8 (Plea Agreement), and admitted to an associated stipulated set of facts. *See* Factual Basis. The Plea Agreement calculated Defendant’s Total Offense Level under the U.S. Sentencing Guidelines at 11, yielding a guideline sentencing range of 8 to 14 months. The Total Offense Level was calculated as follows:

SENTENCING GUIDELINES CALCULATIONS					
<u>Count 1: Unauthorized Disclosure of Tax Records (26 U.S.C. § 7213(a)(1)):</u>					
Base Offense Level (U.S.S.G. § 2H3.1(a)(1))					9
Abuse of Trust Position or Use of Special Skill (U.S.S.G. § 3B1.3)					+2
Obstruction of Justice (U.S.S.G. § 3C1.1)					+2
Acceptance of Responsibility (U.S.S.G. § 3E1.1(a))					-2
Total Offense Level					11
CH Cat. I	CH Cat. II	CH Cat. III	CH Cat. IV	CH Cat. V	CH Cat. VI
8-14	10-16	12-18	18-24	24-30	27-33

Both parties agreed, however, that Amendment 821 to the Sentencing Guidelines—which provides a decrease of two levels for certain individuals with no criminal history—“may result in a reduction of the defendant’s total offense level.” Plea Agreement at ¶ 9(a) & n.1.

In the Plea Agreement, both parties also reserved their respective rights to seek a departure or a variance from the applicable guidelines range. *Id.* at ¶¶ 9(d), 10. In particular, the United States

² The term “return” means “any tax or information return, declaration of estimated tax, or claim for refund required by, or provided for or permitted under, the provisions of this title which is filed with the Secretary by, on behalf of, or with respect to any person, and any amendment or supplement thereto, including supporting schedules, attachments, or lists which are supplemental to, or part of, the return so filed.” 26 U.S.C. § 6103(b)(1). The term “return information” means, as relevant here, “a taxpayer’s identity, the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, overassessments, or tax payments, whether the taxpayer’s return was, is being, or will be examined or subject to other investigation or processing, or any other data, received by, recorded by, prepared by, furnished to, or collected by the Secretary [of the Treasury] with respect to a return or with respect to the determination of the existence, or possible existence, of liability (or the amount thereof) of any person under this title for any tax, penalty, interest, fine, forfeiture, or other imposition, or offense.” 26 U.S.C. § 6103(b)(2)(A).

provided notice that “it expects to seek an upward departure pursuant to Application Note 5 of § 2H3.1 of the Sentencing Guidelines,” *id.* at ¶ 9(d), a provision discussed in further detail below.

At the plea hearing on October 12, 2023, the Court emphasized that “people taking the law into their own hands for any purpose is unacceptable,” ECF No. 13 (Plea Tr.) at 16:19-21, and that “it’s not up to any individual person to decide what law they want to violate or what law they want to follow.” *Id.* at 20:5-7.

On December 20, 2023, the Probation Officer issued a draft PSR. *See* PSR. The PSR is entirely consistent with the Total Offense Level calculated in the Plea Agreement except that it granted Defendant the benefit of Amendment 821, yielding a Total Offense Level of 9 and a guideline sentencing range of 4 to 10 months.

ARGUMENT

The applicable advisory guideline range does not capture the gravity of Defendant’s offense and fails to account for the numerous aggravating factors in this case. Perhaps most centrally, Defendant’s advisory guideline range does not account for the fact that he leaked thousands of individuals’ and entities’ tax returns. His range would be the same today if he had leaked only a single return. For the reasons that follow, a significant term of imprisonment is warranted here and the Court should sentence Defendant to a term of incarceration of 60 months, the statutory maximum.

I. An Upward Departure is Appropriate Under U.S.S.G. § 2H3.1, Application Note 5

First, the Court should grant an upward departure pursuant to Application Note 5 of U.S. Sentencing Guideline § 2H3.1. As relevant here, the Application Note provides that an upward departure may be warranted when the “offense level determined under this guideline substantially understates the seriousness of the offense.” U.S. Sentencing Guideline § 2H3.1, App. Note 5. The

Application Note provides two non-exhaustive examples of circumstances where such a departure would be appropriate: (A) where the offense, as relevant here, “involved personal information, means of identification, . . . or tax return information of a substantial number of individuals” and (B) where the “offense caused or risked substantial non-monetary harm (e.g., physical harm, psychological harm, or severe emotional trauma, or resulted in a substantial invasion of privacy interest) to individuals whose private or protected information was obtained.” *Id.*³

Both examples are squarely applicable here. First, the offense, by its very nature, involved the “tax return information of a substantial number of individuals.” App. Note 5(A). Indeed, as Defendant recently admitted, he disclosed tax return and return information associated with “over a thousand” individuals and entities. Plea Tr. at 11:2-4; *see also* Factual Basis at ¶¶ 10-13. This Application Note example accounts for one of the key aggravating circumstances here: the sheer volume of individuals impacted by Defendant’s crime. In fact, the Court recently allowed the government to pursue an alternative means of victim notification because the “number of potential victims in this case makes it impracticable to provide all of the victims the rights provided under 18 U.S.C. § 3771(a),” the Crime Victims’ Rights Act. ECF No. 5 at 1.

Second, the offense “caused or risked substantial non-monetary harm”—here, “psychological harm” and the “substantial invasion of privacy interest[s]”—to “individuals whose private or protected information was obtained.” App. Note 5(B). Defendant did not merely disclose tax returns. He disclosed information that included income and taxes as well as investments, stock trades, gambling winnings, audit determinations, and many other types of financial material. One of Defendant’s purposes in leaking the tax returns and return information to News Organization 2

³ The Court previously ordered that the parties address whether the number of tax returns Defendant stole and disclosed can be considered at sentencing. Application Note 5(A) provides a straightforward mechanism for the Court to account for the volume of disclosed taxpayer data here.

was to catch the attention of the public with more salacious details than mere tax returns might provide. The “[s]ubstantial invasion of privacy interest[s]” was a core purpose of Defendant’s disclosure scheme. The Court should therefore grant an upward departure under Application Note 5.

II. The 18 U.S.C. § 3553(a) Factors Justify an Upward Variance

Additionally, an upward variance based on the 18 U.S.C. § 3553(a) factors is warranted.

A. The Nature and Circumstances of the Offense

The scope and scale of Defendant’s unlawful disclosures appear to be unparalleled in the IRS’s history. There simply is no precedent for a case involving the disclosure of tax return and return information associated with “over a thousand” individuals and entities. Plea Tr. at 11:2-4; *see also* Factual Basis at ¶¶ 10-13. The immense number of victims here, as discussed above, requires an alternative means of mass victim notification through a government website. ECF No. 5 at 1. And the human impact of Defendant’s crimes is enormous. Many victims have come forward, expressing anger and embarrassment about the exposure of their personal financial information. Worse, it appears that the harm may continue indefinitely: News Organization 2 has continued to publish stories using the data disclosed by Defendant even after the Plea Agreement in this case. Victims who believe their information has only been disclosed to a news organization, but not yet to the general public, have no assurance that their personal information will not be the subject of a news article tomorrow, next week, next month, or even next year. The harm arising from Defendant’s crime is accordingly so extensive and ongoing that it is impossible to quantify.

A second important circumstance of the offense justifying an upward variance is that Defendant’s disclosures were not the result of a single impulse or a momentary lapse in judgement. He executed his disclosure scheme over the course of *multiple years*, plotting and calculating

carefully at each step to minimize the risk of detection and maximize the impact of his disclosures. Indeed, he reorganized his entire life around this crime, reapplying to work at Company A in 2017 “with the goal of getting access to taxpayer information” for Public Official A. PSR at ¶ 16. But it was not until November 2018 that he uploaded Public Official A’s tax returns and not until later the following year that he began disclosing them. PSR at ¶¶ 18-19. The disclosures of Public Official A’s returns and return information continued throughout 2020. PSR at ¶ 20.⁴ But as discussed above, Defendant’s criminal objectives *expanded*: it wasn’t until mid- and late 2020 that he accessed and disclosed the IRS data associated with thousands of individuals. PSR at ¶¶ 21-23. Defendant’s extensive planning and execution over the course of multiple years renders this case unique and deserving of an upward variance.

A third aggravating circumstance justifying an upward variance here is the sophistication and complexity of Defendant’s offense. The convoluted queries Defendant undertook on the Database to camouflage his true criminal purpose; his use of a private website to bypass IRS protocols designed to detect large uploads and downloads; his utilization of unconventional electronic storage devices; and his numerous efforts to conceal his scheme all justify a sentence outside the advisory guidelines range.

B. The Seriousness of the Offense

Defendant’s crime was also very serious. The IRS’s mission, which is to “[p]rovide America’s taxpayers top quality service by helping them understand and meet their tax responsibilities and enforce the law with integrity and fairness to all,” *The Agency, its Mission and Statutory Authority*, Internal Revenue Service, available at <https://www.irs.gov/about-irs/the->

⁴ Defendant’s last known disclosure of Public Official A’s tax returns occurred in Spring 2020, but investigators did not learn of his responsibility for these disclosures until more than three years later.

agency-its-mission-and-statutory-authority, cannot be achieved without faith that IRS employees and contractors like Defendant will safeguard citizens' private information. Defendant's crime has undermined public faith and confidence in the IRS, an institution that is critical to the effective functioning of our government.

Moreover, Defendant's offense constitutes an egregious breach of the trust placed in him by our government. The IRS provided Defendant with access to sensitive, unmasked data associated with millions of Americans. Factual Basis at ¶¶ 3-4; PSR at ¶ 13. Instead of respecting the trust that the agency (and, by extension, hundreds of millions of individuals who shared their information with it) placed in him, Defendant exploited it to advance his own private, political agenda. An upward variance is appropriate to communicate to the public that such breaches of trust will not be tolerated under a system of laws that obligates citizens to disclose their financial information to the government.

Finally, as the Court recognized during the plea hearing, *see* Plea Tr. at 16, Defendant essentially chose to take the law into his own hands: his disclosures were in fact part of a lawless, vigilante effort to circumvent the democratic process. That very process ultimately led to the legal release of Public Official A's tax returns. *See* Marianna Sotomayor et al., *House Panel Releases Trump Tax Returns in Another Setback for Former President*, Washington Post (Dec. 30, 2022). And there were countless legitimate opportunities for Defendant to address what he perceived as an unjust tax system without surreptitiously abusing the public trust for years; covering his tracks by deleting and destroying data; and hiding purloined tax returns on an iPod.

C. Defendant's History and Characteristics

Defendant's history and characteristics, too, justify an upward variance. He has a loving family, he attended and graduated from college, he started a successful business, and he served as

an effective consultant at Company A. PSR at ¶¶ 50-55, 67-70, 73. Defendant was a sophisticated professional who received specialized training for years on the proper handling of tax information. Factual Basis at ¶ 4; PSR at ¶ 13. Based on his training, his personal experience, and his work, he understood the gravity of his offense. He understood the impact that it would have on his victims. But he acted anyway.

D. The Need for General Deterrence

Finally, the Court should grant an upward variance to send a message to other individuals like Defendant who have been entrusted with Americans' private taxpayer information. Individuals like Defendant, motivated by ideology or politics or economic gain, may weigh the prospect of a sentence like the one contemplated by the advisory guideline range here against the perceived benefits of disclosure. Perhaps that is what Defendant did. The Court should exercise its discretion to dissuade such calculus, compelling individuals under such circumstances to consider the likelihood of a lengthy term of incarceration.

It may well be that the sentences handed down under somewhat similar circumstances have inadequately accounted for the seriousness of ideologically motivated leaks. For example, in one recent case, an IRS analyst accused of leaking Suspicious Activity Reports (SARs) associated with a prominent attorney received a probationary sentence. *See IRS Worker Who Leaked Cohen Docs Sentenced to Five Years Probation*, Courthouse News Service, <https://www.courthousenews.com/irs-worker-who-leaked-cohen-docs-sentenced-to-five-years-probation/> (Jan. 17, 2020); *United States v. John C. Fry*, Case No. 19-CR-102 (N.D. Cal.). In another, an employee of the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) was sentenced to six months in prison for leaking thousands of SARs and other materials containing sensitive personal and financial information to a reporter, purportedly because

she believed that FinCEN engaged in wrongdoing. *See Press Release: Former Senior FinCEN Employee Sentenced to Six Months in Prison for Unlawfully Disclosing Suspicious Activity Reports*, U.S. Attorney's Office for the Southern District of New York, <https://www.justice.gov/usao-sdny/pr/former-senior-fincen-employee-sentenced-six-months-prison-unlawfully-disclosing> (June 3, 2021); *United States v. Natalie Mayflower Sours Edwards*, Case No. 19-CR-64 (S.D.N.Y.). Although tax returns and return information enjoy stronger statutory and privacy protection than SARs, the advisory sentencing guidelines applicable here still do not adequately capture the severity of offenses like this one.

The Court may also look to similar cases involving the disclosure of classified information to journalists. For example, in one recent case, an employee of the Defense Intelligence Agency was sentenced to 30 months in prison after pleading guilty to communicating Top Secret/Sensitive Compartmented Information, primarily over the telephone, to two reporters. *See Press Release: Former DIA Analyst Sentenced for Leaking Classified Information to Journalists*, U.S. Department of Justice, <https://www.justice.gov/opa/pr/former-dia-analyst-sentenced-leaking-classified-information-journalists> (June 18, 2020); *United States v. Henry Kyle Frese*, Case No. 19-CR-304 (E.D. Va.). In another, a contractor with the National Security Agency was sentenced to 63 months in prison after pleading guilty to searching for, identifying, and printing a single classified intelligence report and mailing it to a news organization. *See Press Release: Federal Government Contractor Sentenced for Removing and Transmitting Classified Materials to a News Outlet*, U.S. Department of Justice, <https://www.justice.gov/opa/pr/federal-government-contractor-sentenced-removing-and-transmitting-classified-materials-news> (Aug. 23, 2018); *United States v. Reality Leigh Winner*, Case No. 17-CR-34 (S.D. Ga.).

At bottom, 18 U.S.C. § 3553(a)(2)(B) obligates the Court to consider the need for the sentence imposed to “afford adequate deterrence to criminal conduct” and provides a statutory vehicle for the Court to communicate an appropriate message about the seriousness of disclosing taxpayer data.

CONCLUSION

For the foregoing reasons, the United States requests that the Court sentence Defendant to a term of incarceration of 60 months.

Dated: January 16, 2024

Respectfully submitted,

COREY R. AMUNDSON
Chief, Public Integrity Section
Criminal Division
U.S. Department of Justice

BY:
/s/ Jonathan E. Jacobson
JENNIFER A. CLARKE
Deputy Chief
JONATHAN E. JACOBSON
Trial Attorney
Public Integrity Section
United States Department of Justice
1301 New York Avenue, NW
Washington, DC 20530
Telephone: (202) 514-1412

CERTIFICATE OF SERVICE

I hereby certify that on the 16th day of January 2024, I caused the foregoing to be electronically filed with the Clerk of the Court using the CM/ECF System, which will then send a notification of such filing to all attorneys of record.

/s/ Jonathan E. Jacobson
Jonathan E. Jacobson
Trial Attorney, Public Integrity Section
U.S. Department of Justice
1301 New York Ave. NW, 10th Fl.
Washington, DC 20530
Tel: 202-514-1412
Email: Jonathan.Jacobson@usdoj.gov