INSTITUTE FOR
FREE SPEECH

December 9, 2019

Via Electronic Submission System

Victoria Judson
Associate Chief Counsel
Office of the Associate Chief Counsel
(Employee Benefits, Exempt Organizations, and Employment Taxes)
Internal Revenue Service
111 Constitution Avenue, NW
Washington, DC 20224

RE: Comments on REG-102508-16: Guidance Under Section 6033 Regarding the Reporting Requirements of Exempt Organizations

Dear Ms. Judson:

On behalf of the Institute for Free Speech, I respectfully submit the following supplemental comments in support of the proposed rule updating the information reporting regulations under Section 6033. Specifically, I write to discuss two issues raised by other commentators: (1) the suggestion that adoption of the rule will encourage foreign interference in American elections and (2) that providing donor information to the Service imposes few inherent costs.

Foreign Spending in Elections

A few commentators have claimed, without evidence, that the proposed rule would "invite illegal foreign spending in U.S. elections" and otherwise encourage unlawful meddling by non-U.S. persons in the nation's political debates.[1] They assume, again without any evidence, that the Internal Revenue Service's ("IRS" or "Service") reporting requirements, specifically Form 990, Schedule B, stops the spending of illegal foreign money on election campaigns. The claim is unfounded and provides no principled or practical basis for rejecting the proposed rule.

Schedule B quite simply does not serve the purpose these commentators propose. As has been explained elsewhere,[2] it is a tool for the administration and enforcement of tax laws.

[1] *See, e.g.*, Campaign Legal Center, Comment on REG-102508-16: Guidance Under Section 6033, Regarding the Reporting Requirements of Exempt Organizations at 1-4, (Dec. 5, 2019) ("CLC Comments"), https://www.regulations.gov/document?D=IRS-2019-0039-3096.

[2] *See* Public Policy Legal Institute, Comments of the Public Policy Legal Institute on Guidance Under Section 6033 Regarding the Reporting Requirements of Exempt Organizations at 1, (Dec. 6, 2019), https://www.regulations.gov/contentStreamer?documentId=IRS-2019-0039-

It was not intended by Congress, or the Service, to supplant the mission of the Federal Election Commission and other entities with the mission of enforcing campaign finance restrictions. Moreover, the proposed use of Schedule B simply does not work as a practical matter.

- Tax-exempt organizations may legally accept foreign money, as long as they do not use the funds to influence federal elections. Therefore, the mere reporting of contributions from a foreign donor on an IRS form would have no significance. While very few tax-exempt organizations have significant foreign contributions, so long as such donations are segregated, even those groups may spend money on federal campaign activities, as long as U.S. citizens make the decisions. Unless the proposal is to use the mere presence of foreign contributions as the basis for invasive investigations and audits, which would raise potentially serious legal objections, Schedule B does little to capture illicit activity.

- If foreigners are going to launder money into federal elections, they are not going to use a foreign address on a tax-exempt organization's return. Even assuming the IRS received self-incriminating information on a tax form, unless the amount of foreign contributions exceeds the amount spent by the group for non-political activities using other funds, one cannot simply assume that any of the foreign gifts were spent to influence elections.

- In any event, the IRS would have no reason to analyze such spending. The IRS has no authority or responsibility for enforcing campaign finance laws. Additionally, except in very limited circumstances in which there is actual evidence of a criminal act, the tax privacy laws generally prevent the IRS from sharing the donor information in Schedule B with the two agencies that *do* enforce campaign finance laws: the Federal Election Commission and the Department of Justice. Those agencies have other effective methods for obtaining such information from third parties.

- Using a donor's surname or foreign address to suggest he or she is not an American citizen raises deep concerns. As the Service well knows, many Americans reside abroad. And the enforcement of tax laws based upon the perceived ethnic or geographical origin of a person's name raises constitutional objections that reach far beyond the First Amendment.

The Risk of Disclosure

At least one commenter suggests "the risk of inadvertent public disclosure is minute."[3] But its only evidence is the opinion of a federal appellate court discussing the risk of

4924&attachmentNumber=1&contentType=pdf, ("the ONLY intended purpose of Schedule B is the administration of tax laws, not campaign finance proposals…") (emphasis removed).

[3] CLC Comments at 4-7.

Schedule B disclosure by the California Department of Justice, not the Service.[4] In any event, that court decision acknowledged a "risk of inadvertent public disclosure based on past confidentiality lapses," although it ultimately discounted that risk.[5] That ruling was highly controversial, drawing a vigorous opposing opinion from five judges.[6] Nor is that decision final; it is presently the subject of a petition to the U.S. Supreme Court for a writ of *certiorari*.

The five-judge dissent noted that "[a]lthough the state is required to keep [Schedule B] donor names private, the district court found that the state's promise of confidentiality was illusory. The state's database was vulnerable to hacking and scores of donor names were repeatedly released to the public, even up to the week before trial."[7]

Later, the dissenting opinion summarized the lower court's findings, which capture the very substantial risks to which nonprofit organizations are exposed by Schedule B disclosure requirements:

> The evidence produced at trial in this case provided…ample evidence of human error in the operation of the state's system. State employees were shown to have an established history of disclosing confidential information inadvertently, usually by incorrectly uploading confidential documents to the state website such that they were publicly posted. Such mistakes resulted in the public posting of around 1,800 confidential Schedule Bs, left clickable for anyone who stumbled upon them. And the public did find them. For instance, in 2012 Planned Parenthood become aware that a complete Schedule B for Planned Parenthood Affiliates of California, Inc., for the 2009 fiscal year was publicly posted; the document included the names and addresses of hundreds of donors.
>
> There was also substantial evidence that California's computerized registry of charitable corporations was shown to be an open door for hackers. In preparation for trial, the plaintiff asked its expert to test the security of the registry. He was readily able to access every confidential document in the registry—more than 350,000 confidential documents—merely by changing a single digit at the end of the website's URL. When the plaintiff alerted California to this vulnerability, its experts tried to fix this hole in its system. Yet when the expert used the exact same method the week before trial to test the registry, he was able to find 40 more Schedule Bs that should have been confidential.[8]

In the past, all government records were on paper and stored in physical filing cabinets. Accordingly, a significant theft of confidential information was difficult to accomplish.

---

[4] *Ams. for Prosperity Found. v. Becerra*, 919 F.3d 1177 (9th Cir. 2019) (*en banc*) (denying *en banc* review of *Ams. for Prosperity Found. v. Becerra*, 903 F.3d 1000 (9th Cir. 2018), which upheld California's Schedule B collection regime).
[5] *Id*. at 1192.
[6] *Ams. for Prosperity Found.*, 919 F.3d at 1178-1187 (Ikuta, J., dissenting).
[7] *Id.* at 1178.
[8] *Id.* 1184-1185 (internal citations omitted).

Today, so-called "thumb drives" can store over 75 million pages of information. And information can simply be culled from or sent out of a networked system with inadequate security protections.

Additionally, the IRS now provides Form 990 information for every organization that files a Form 990 in a bulk download. If the IRS were to err, as it has done in the past, and include confidential information in that bulk download, the information can never be retrieved from the public domain. This is especially true since at least one organization that republishes this bulk data is "an independent, nonprofit newsroom" specializing in investigative journalism.[9]

Moreover, in recent years the federal government has been vulnerable to leaks of highly confidential information, even vital national security information. Leaks are possible through hacking or employees or contractors who download confidential bulk data onto small storage devices and then give it to journalists or websites for publication.

As noted in the indictment of Julian P. Assange, "[Chelsea] Manning downloaded four nearly complete databases from departments and agencies of the United States. These databases contained approximately 90,000 Afghanistan war-related significant activity reports, 400,000 Iraq war-related significant activities reports, 800 Guantanamo Bay detainee assessment briefs, and 250,000 U.S. Department of State cables. The United States had classified many of these records up to the SECRET level pursuant to Executive Order No. 13526 or its predecessor orders."[10] Many of these documents later obtained by Manning were published on the WikiLeaks website.

Other agencies entrusted with sensitive data have nevertheless proven they are vulnerable to infiltration by nefarious hackers. As security expert Michael Adams correctly observed, the 2015 "Office of Personnel Management ('OPM') data breach involve[d] the greatest theft of sensitive personnel data in history."[11] In sum, "[a]mong the sensitive data that was exfiltrated were millions of SF-86 forms, which contain extremely personal information gathered in background checks for people seeking government security clearances, along with records of millions of people's fingerprints."[12]

Like these other government agencies, the IRS has also been a tempting target for abuse. Last year, a high ranking official at the Treasury Inspector General for Tax Administration ("TIGTA") testified before Congress and explained that "in May 2015,

---

[9] "About Us," ProPublica, https://www.propublica.org/about/. ProPublica notes that you "can browse IRS data released since 2013 and access more than 14 million tax filing documents going back as far as 2001" via its page. "Nonprofit Explorer," ProPublica, https://projects.propublica.org/nonprofits.

[10] Superseding Indictment at 5, ¶ 12, *United States v. Assange*, Case No. 18-111 (E.D. Va. May 23, 2019) (bold removed), https://www.justice.gov/opa/press-release/file/1165556/download.

[11] Michael Adams, "Why the OPM Hack Is Far Worse Than You Imagine," Lawfare, March 11, 2016, https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine.

[12] Josh Fruhlinger, "The OPM hack explained: Bad security practices meet China's Captain America," CSO, Nov. 6, 2018, https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

the IRS discovered that criminals used taxpayers' personal identification information obtained from sources outside the IRS to impersonate the taxpayers and gain unauthorized access to tax information…TIGTA believes that the system was widely exploited by numerous bad actors who collectively made at least 724,000 potentially unauthorized accesses to taxpayer accounts, resulting in the filing of 252,400 potentially fraudulent tax returns and the issuance of $490 million in potentially fraudulent refunds."[13]

TIGTA also publishes an "Annual Assessment of the Internal Revenue Service's Information Technology Program." The most recent report revealed that "[p]roblems were…reported in the IRS's handling of the privacy of taxpayer data, system access controls, system environment security, disaster recovery, separation of duties, system security and privacy training, and system security documentation."[14] The report determined that "taxpayer data will remain vulnerable to inappropriate and undetected use, modification, or disclosure until all areas of the IRS security program are fully implemented in compliance with the requirements of the Federal Information Security Modernization Act of 2014."[15]

Put simply, the government has not demonstrated an infallible ability to maintain the confidentiality of information in its care, including highly-sensitive data which it is highly motivated to protect. Under such circumstances, the Service should collect only that information it actually needs for its actual mission. The narrow opinion of a single appellate court, considering a different rule in a different context, does little to undermine this overarching point.

Political Polarization and the Risks of Disclosure

A 2017 poll by the Associated Press-NORC Center for Public Affairs Research found that "more than half of Americans say the political polarization of the nation is extremely or very threatening, and another 34 percent say it is moderately threatening" to the American way of life.[16]

Part of that threat comes from how a polarized polity encourages partisans to target and vilify perceived partisan or ideological opponents. As noted in a recent opinion by Judge Brian R. Martinotti of United States District Court for the District of New Jersey, there is now a climate where "the so-called cancel or call-out culture that has resulted in people

[13] Testimony of Michael E. McKenney, Deputy Inspector General for Audit, Treasury Inspector General for Tax Administration at 2, "The Internal Revenue Service's Taxpayer Online Authentication Efforts," Committee on Ways and Means, Subcommittee on Oversight. September 26, 2018, https://www.treasury.gov/tigta/congress/congress_09262018.pdf.

[14] Treasury Inspector General for Tax Administration, "Highlights," Annual Assessment of the Internal Revenue Service's Information Technology Program for Fiscal Year 2019, September 27, 2019, available at https://www.treasury.gov/tigta/auditreports/2019reports/201920083fr.pdf.

[15] *Id*.

[16] "The American Identity: Points of Pride, Conflicting Views, and a Distinct Culture," Associated Press-NORC Center for Public Affairs Research, http://apnorc.org/projects/Pages/HTML%20Reports/points-of-pride-conflicting-views-and-a-distinct-culture.aspx.

losing employment, being ejected or driven out of restaurants while eating their meals; and where the Internet removes any geographic barriers to cyber harassment of others."[17] Thus, merely by collecting donor information and risking its accidental or nefarious disclosure, the Service will impose a potential chill on giving to tax-exempt organizations.

Accordingly, the Service should be especially sensitive to safeguarding the privacy of donor information where individuals and politically-active groups clearly seek that information in order to deter contributions to their political opponents. The best way to protect privacy of association and belief is to avoid collecting sensitive information unless that data is absolutely essential to the Service's core mission. The current use of Schedule B does not meet that standard.

* * *

In conclusion, the risks of unauthorized disclosure are unknown. But such disclosures have the potential to reveal enormous amounts of confidential information and could inflict serious harm on free speech and association. The IRS should adopt the proposed rule.

Respectfully submitted,

Allen Dickerson
INSTITUTE FOR FREE SPEECH
124 S. West Street, Suite 201
Alexandria, VA 22314

[17] *Ams. for Prosperity Found v. Grewal*, 2019 U.S. Dist LEXIS 170793, Case No. 19-14228 (D.N.J. Oct. 2, 2019).