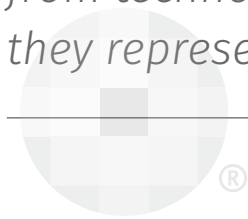


Do IRS Computers Dream About Tax Cheats? Artificial Intelligence and Big Data in Tax Enforcement and Compliance

By Carina Federico and Travis Thompson*

Carina Federico and Travis Thompson explore the nature of artificial intelligence and big data, how the IRS uses and benefits from technology, and what tax practitioners should know when they represent clients in the future.



Wolters Kluwer

Introduction

If tax practitioners continue to rely upon television and movies to guide their understanding about artificial intelligence, they will surely be at a disadvantage. Machines are not taking over the world. Computers do not have minds and they do not dream.

But, even though computers have certain subjective limitations, they have unlimited potential in the modern tax enforcement and compliance initiatives recently adopted by the IRS. As federal enforcement agencies are increasingly asked to do more with less, the U.S. government has implemented advanced technology platforms to enforce financial crimes which have increased in sophistication. As tax cheats and other financial criminals started targeting the digital world, the IRS reciprocated those efforts by modernizing its tax enforcement and compliance strategy.

This article explores the nature of artificial intelligence and big data, how the IRS uses and benefits from technology, and what tax practitioners should know when they represent clients in the future.

What Is Artificial Intelligence and Big Data?

A simple definition of artificial intelligence is “machines acting in ways that seem intelligent.”¹ But the term artificial intelligence is not so easy to define.

CARINA FEDERICO is an Associate in Crowell & Moring’s Tax Group and resident in the firm’s Washington, D.C. office. **TRAVIS THOMPSON** is an Associate in the Tax and Criminal Defense practice groups at Sideman & Bancroft, LLP in San Francisco, California.

The word “artificial” simply means something that does not occur naturally. But the word “intelligence” has been defined in many ways. One good definition, by psychologist Howard Gardner, focuses on problem-solving. Gardner explained, “intelligence is the ability to solve problems, or to create products, that are valued within one or more cultural settings.”²

An important distinction in the field of artificial intelligence is between “narrow A.I.” and “general A.I.” Narrow A.I. is defined as “machine-based systems designed to address a specific problem (such as playing chess).”³ To date, all applications of artificial intelligence are examples of narrow A.I. In contrast, general A.I. refers to machines with the ability to solve many different types of problems on their own, like humans can. Examples of this are usually seen in science fiction when computers and machines become self-realized and take over the world. General A.I. is currently a hot research topic, but many scientists argue it never will become reality.⁴

Currently, organizations use three types of narrow A.I.: machine learning, natural language processing, and robotics.⁵ Robots are automated devices that perform physical tasks in the real world.⁶ Natural language processing is technology that enables machines to understand and generate language in its written and spoken form (think Microsoft Word spellcheck or Google translate).⁷ Finally, machine learning artificial intelligence uses predictive computer programs that automate learning through experience using large data sets.⁸ The artificial intelligence technology used by the IRS is a form of machine learning technology, although the IRS is currently testing natural language processing applications.⁹

The rise of big data has increased the need for large scale organizations like the IRS to rely upon machine learning technology platforms. The artificial intelligence and big data explosion are happening for specific reasons. First, technological advances have allowed for cheaper and more efficient storage of the 2.5 quintillion bytes of data that are produced daily around the world.¹⁰ Given this explosion of data production, 90% of the world’s data has been created in the last two years.¹¹ Data are created through every digital process from electronic transactions to cell phones to social media to live video feeds.¹² All of this is big data.

Second, computing power and the speed of computation is the fastest it has ever been.¹³ This makes it easier to train artificial intelligence-based systems because the more data the artificial intelligence has to compute, the more reliable artificial intelligence becomes.¹⁴ Among the U.S.

government agencies, the IRS likely has one of the largest troves of data for artificial intelligence to compute.

How Will Artificial Intelligence and Big Data Impact IRS Enforcement Efforts?

Simply put, the IRS’s use of artificial intelligence and big data has dramatically improved the efficiency of the agency, specifically the agency’s employees.¹⁵ The IRS has implemented a data-driven mindset throughout the organization by increasing visibility and awareness for its employees of the availability of Big Data within the organization.¹⁶ With limited resources and reduced budgets, artificial intelligence and big data allow IRS agents to work faster and smarter.¹⁷

Using data and predictive analytics, the IRS can discover useful information about taxpayers faster and more efficiently during the audit or criminal investigation period, which helps support decision making and impacts case selection for all jurisdictions.¹⁸ This also leads to better coordination among other law enforcement and federal agencies because these agencies are able to fuse large tax and financial data with other gathered data sets to investigate cases more thoroughly, and de-conflict other data by resolving contradictory conclusions during the investigation process.¹⁹

Research, Applied Analytics and Statistics

In 2011, the IRS created the Office of Compliance Analytics (“OCA”) in order to construct analytics programs that could identify potential refund fraud, detect taxpayer identity theft, and handle non-compliance issues efficiently.²⁰ OCA was charged with developing an advanced analytics program that would rely on the use of big data and predictive algorithms to reduce tax fraud.²¹ In 2016, significant organizational changes took place when OCA and Research, Analysis and Statistics (“RAS”) merged to create the office of Research Applied Analytics & Statistics (“RAAS”).²²

The mission of RAAS is to lead a data-driven culture through innovative and strategic research, analytics, statistics, and technology services in partnership with internal and external stakeholders.²³ Combining artificial intelligence and advanced analytics platforms, RAAS extracts value by leveraging vast amounts of proprietary data stored within the IRS legacy computers.²⁴ Using

sophisticated data graphing techniques, RAAS's approach improves traditional IRS methods because its various departments can now find complex relationships within existing data sets which were previously unknown to IRS enforcement agents.²⁵ These findings then are shared with IRS employees to improve taxpayer compliance, detect and prevent fraudulent behavior, and improve enforcement efforts.²⁶

Nationally Coordinated Investigations Unit

IRS Criminal Investigations created the Nationally Coordinated Investigations Unit (NCIU), which is entirely focused on data analytics.²⁷ NCIU employs an analytic platform for financial and tax criminal case development that is used by over 2,000 analysts and agents within the department.²⁸ This analytic platform increases the speed of investigation by providing increased efficiency in user workflows, reducing tasks that used to take hours to minutes, and building out leads in days rather than weeks and months. The IRS announced that due to its success, NCIU will become an official CI section in 2019, which will hire additional personnel and launch new initiatives.²⁹

During the past several years, the IRS-CI unit successfully used these data analytics tools in its efforts to takedown numerous dark Web marketplaces and illicit exchanges.³⁰ RAAS helps the IRS define issues using large data sets, conduct exploratory analysis, support case development, and help deter future non-compliance.

NCIU's use of data analytics has also improved the quality of new lead generation by providing agents and analysts with the ability to generate high value leads from millions of FinCEN reports and other data sources.³¹ Finally, these new tools help IRS CI build larger cases and identify additional losses to the government, leading to more complete case assessments.

Cryptocurrency Enforcement

The IRS now considers cryptocurrency an "emerging and emerged-threat."³² For criminal tax enforcement purposes, the IRS is focused on how cryptocurrency holders may be avoiding the payment of capital gains tax on the sale of cryptocurrencies, or using offshore crypto-accounts to escape foreign bank account reporting requirements.³³ All significant crypto-cases are now assigned an IRS Special Agent, and the IRS now has the finest expertise in the world tracking cryptocurrency.³⁴

Administratively, the IRS has made strides to educate staff and put infrastructure in place to enforce cryptocurrency transactions. Two major IRS cryptocurrency groups now exist in Los Angeles and Washington D.C. Every IRS office in the United States is staffed with a cyber-crimes employee, and the IRS implemented mandatory training for all IRS Criminal Investigation employees on cryptocurrency.³⁵

The IRS is getting results on its cryptocurrency enforcement efforts because of its close collaboration with other agencies, including the Department of Justice and international enforcement agencies, to track down "abuses of cryptocurrency accounts."³⁶ The IRS has tens of millions of records from various investigations and is making connections to select new cases. Significant resources are spent on cryptocurrency investigations and taxpayers should be mindful of that.³⁷

Sophisticated Methods to Select Returns for Audit

The IRS used data analytics for years to select returns for audit, but the new technology has significantly improved the IRS's abilities. In September 2018, the IRS signed a deal with Palantir Technologies for \$99 million over seven years.³⁸ Palantir Gotham is a project under the Palantir Technologies umbrella with many other government clients, including the CIA and Department of Defense.³⁹ Palantir's platforms are used to "integrate[] and transform[] data, regardless of type or volume, into a single, coherent data asset ... [that is] mapped into meaningfully defined objects—people, places things, and events—and the relationships that connect them."⁴⁰

The IRS uses the Palantir Gotham platform to run its Lead Case Analytics service. Special agents and investigative analysts in IRS Criminal Investigations use Lead Case Analytics to "generate leads, identify schemes, uncover tax fraud, and conduct money laundering and forfeiture investigative activities."⁴¹

Although Lead Case Analytics and other data analytics tools are relatively new to the IRS, the IRS has used data for decades to determine which tax returns it will select for audit. For instance, the IRS has used its Discriminate Inventory Function System (DIF) since the 1960s.⁴² The DIF system assigns a numeric score to individual and some corporate tax returns; higher DIF scores indicate a higher likelihood that a return will be audited and result in a change to the taxpayer's tax liability.⁴³ The IRS also selects returns for examination based on information received through third-party reporting, such as Forms 1099 and W-2.⁴⁴ Lead Case Analytics essentially uses the

same framework and methods that the IRS has always used, but on steroids.

The information collected and analyzed by the IRS will continue to be massive and varied. New technology will allow the IRS to use data more efficiently and in more sophisticated ways.

The IRS's Future Plans

In the last year, the IRS has taken significant steps to enhance its technological capabilities. On June 27, 2018, the IRS's Cybersecurity issued a Request for Information seeking input from the industry regarding artificial intelligence, machine learning, cognitive computing, and data analytics techniques, algorithms, and capabilities that have application to cybersecurity areas in the IRS.⁴⁵ On December 4, 2018, the IRS revised the Request for Information⁴⁶ and posted an attachment listing five use cases that the IRS is looking to address: (1) analyzing user behavior to detect potentially suspicious patterns by using A.I. and machine learning-driving systems; (2) analyzing network traffic to pinpoint trends indicating potential attacks; (3) incident response integration and management to accelerate the discovery of software or device vulnerabilities; (4) preemptive social media threat analysis to monitor social media channels including comments and posts to detect threats against IRS systems; and (5) application security penetration testing which identify threats. Responses to the request were due on January 4, 2019, so the IRS may announce soon the use of new platforms and technologies based on the responses it has received to its request.

On December 18, 2018, the IRS issued a Request for Information regarding tools that could be used for social media research.⁴⁷ In its request, the IRS states:

Business and individuals increasingly use social media to advertise, promote, and sell products and services ... Most of this information is unrestricted, allowing the public, businesses, and various government agencies to discover taxpayers' location and income sources. But the IRS currently has no formal tool to access this public information, compile social media feeds, or search multiple social media sites. The IRS's hope is that a vendor-supplied tool would help expedite IRS case resolution for existing compliance cases, providing a more efficient way of identifying resources and assisting with the collection of known tax deficiencies, leading to increased collection of revenue involving unfiled tax returns and other tax liabilities.⁴⁸

The IRS explains that it will only use the tool to "assist with previously identified tax compliance cases" and will not use the tool "to search internet or social media sites for purposes of initiating new tax audits."⁴⁹ The IRS's use of social media data likely will raise concerns with privacy issues despite the IRS's statement that it won't use the data to go out looking for new audits and enforcement actions.

What Tax Practitioners Should Know

Armed with the knowledge that the IRS is and will continue to use new and better technology to aid in tax enforcement, what can tax practitioners do to better prepare their clients who are under audit or may be subject to a criminal investigation?

First, tax practitioners should ensure that their clients are as open and honest as possible with them so that practitioners are prepared to address issues raised by the IRS in audit and during interviews with IRS agents. Practitioners need to develop new questions and be mindful of the IRS's new technological capabilities when interviewing new clients. Client intake questions should include inquiries about social media usage and online sales through digital marketplaces, at a minimum. It is imperative that modern tax practitioners develop a full understanding of a client's digital footprint.

The IRS is unlikely to tell taxpayers what information they already have, and where and how they have obtained information about the taxpayer, so the only way a tax practitioner will be able to assist the client is if the client gives them the information they need to handle whatever issues arise. The IRS does not need to disclose to the taxpayer the "standards used or to be used for the selection of returns for examination, or data used or to be used for determining such standards."⁵⁰

Second, practitioners should advise clients to be mindful about what they post on social media. For instance, a taxpayer should not tell the IRS that they do not have any money, but then post pictures of himself on Instagram with expensive cars or on an extravagant vacation. The IRS has announced a desire to get its hands on social media data, and when it does, it will use the data collected to determine when taxpayers are being untruthful.

Lastly, tax practitioners should follow developments in technology to stay abreast of changes at the IRS. The IRS appears to have fully committed to the use of artificial intelligence and machine learning and will continue to add new technology to its enforcement arsenal in years to come.

ENDNOTES

- * Title inspired by Philip K. Dick, *Do Androids Dream of Electric Sheep* (1968) (later adapted into the movie “Blade Runner”). Carina focuses her practice on federal tax controversy and tax litigation matters before the IRS and in trial and appellate courts across the United States. Carina previously was a trial attorney at the U.S. Department of Justice, Tax Division, where she represented the IRS as lead counsel in civil actions, contested matters, and adversary proceedings. At the Department of Justice, Carina was awarded the Tax Division’s Outstanding Attorney Award in 2014 and a Special Commendation in 2013. She also served as deputy associate counsel for the White House, where she was the tax counsel on the vetting team for presidential nominations. Travis handles all aspects of taxpayer controversies against the Internal Revenue Service and State of California, and represents clients in litigation in the U.S. Tax Court, U.S. District Courts, U.S. Courts of Appeals, and California state courts. He has drafted petitions for Writ of Certiorari to the U.S. Supreme Court and represents clients in various white collar criminal defense cases. Travis advises clients on the tax consequences of Bitcoin and cryptocurrency transactions and consults with clients on how artificial intelligence impacts modern business strategy and domestic and international tax compliance.
- ¹ MIT Sloan School of Management & MIT Computer Science and Artificial Intelligence Laboratory (CSAIL), *Artificial Intelligence: Implications for Business Strategy*, Module 1 Unit 2 Casebook (2017).
- ² Howard Gardner, *Theory of Multiple Intelligence* (1983).
- ³ MIT Sloan School of Management & MIT Computer Science and Artificial Intelligence Laboratory (CSAIL), *Artificial Intelligence: Implications for Business Strategy*, Module 1 Unit 2 Casebook (2017).
- ⁴ *Id.*
- ⁵ *Id.*
- ⁶ *Id.*
- ⁷ *Id.*
- ⁸ *Id.*
- ⁹ “The IRS’s Modern Use of Artificial Intelligence and Big Data for Tax Enforcement,” American Bar Association Section on Taxation Webinar (Dec. 5, 2018).
- ¹⁰ IBM, *Bringing Big Data to the Enterprise*, available at www-01.ibm.com/software/in/data/bigdata/.
- ¹¹ Kimberly Houser & Debra Sanders, *The Use of Big Data Analytics by the IRS: What Tax Practitioners Need to Know*, 128 J. TAXATION 16 (Feb. 8, 2018). Thomas Reuters/Tax & Accounting.
- ¹² *Id.*
- ¹³ MIT Sloan School of Management & MIT Computer Science and Artificial Intelligence Laboratory (CSAIL), *Artificial Intelligence: Implications for Business Strategy*, Module 1 Unit 2 Casebook (2017).
- ¹⁴ *Id.*
- ¹⁵ Eric Hylton, Deputy Chief of Internal Revenue Service Criminal Investigations, Address at American Bar Association Section of Taxation Tax Practice Management Panel, Hyatt Regency Atlanta, GA (Oct. 5, 2018).
- ¹⁶ *Id.*
- ¹⁷ *Id.*
- ¹⁸ *Id.*
- ¹⁹ *Id.*
- ²⁰ Kimberly Houser & Debra Sanders, *The Use of Big Data Analytics by the IRS: What Tax Practitioners Need to Know*, 128 J. TAXATION 16 (Feb. 8, 2018). Thomas Reuters/Tax & Accounting.
- ²¹ *Id.*
- ²² IRM 1.1.18 (Sept. 28, 2018).
- ²³ IRM 1.1.18.1(1) (Sept. 28, 2018). RAAS is headed by a Chief Research and Analytics Office who reports directly to the Deputy Commissioner of Operations Support. The Chief Research and Analytics Office is responsible for the oversight and coordination of the activities of RAAS’s five divisions: (1) Data Exploration and Testing; (2) Data Management; (3) Knowledge Development and Application; (4) Statistics and Income; and (5) Strategy and Business Solutions.
- ²⁴ IRM 1.1.18.1(2) (Sept. 28, 2018).
- ²⁵ IRM 1.1.18.1.1 (Sept. 28, 2018).
- ²⁶ IRM 1.1.18.1.1(1) (Sept. 28, 2018).
- ²⁷ IRS, Criminal Investigation Annual Report (2018), available at www.irs.gov/pub/irs-utl/2018_irs_criminal_investigation_annual_report.pdf.
- ²⁸ *Id.*
- ²⁹ *Id.*
- ³⁰ Don Fort, Chief of Internal Revenue Service Criminal Investigations, Address at American Bar Association Section of Taxation Criminal and Civil Tax Penalties Panel, Grand Hyatt Washington D.C. (May 12, 2018).
- ³¹ IRS, Criminal Investigation Annual Report (2018), available at www.irs.gov/pub/irs-utl/2018_irs_criminal_investigation_annual_report.pdf.
- ³² Don Fort, Chief of Internal Revenue Service Criminal Investigations, Address at American Bar Association Section of Taxation Criminal and Civil Tax Penalties Panel, Grand Hyatt Washington D.C. (May 12, 2018).
- ³³ *Id.*
- ³⁴ *Id.*
- ³⁵ *Id.*
- ³⁶ *Id.*
- ³⁷ *Id.*
- ³⁸ IRS Contract Proposal, Performance Work Statement, Jan. 11, 2017, at 1. The IRS has worked with Palantir since 2013. Siri Bulusu, *Palantir Deal May Make IRS “Big Brother-ish” While Chasing Cheats*, BLOOMBERG TAX, Nov. 15, 2018.
- ³⁹ Lizette Chapman, *Peter Thiel’s Palantir Wins \$876 Million U.S. Army Contract*, Mar. 9, 2018, 2:39 PM, available at www.bloomberg.com/news/articles/2018-03-09/peter-thiel-s-palantir-wins-876-million-u-s-army-contract; Siobhan Gorman, *How Team of Geeks Cracked Spy Trade*, WALL ST. J., Sept. 4, 2009.
- ⁴⁰ Palantir Gotham, www.palantir.com/palantir-gotham/ (last visited Mar. 12, 2018).
- ⁴¹ Internal Revenue Service, Privacy Impact Assessment: Lead Case Analysis, LCA (July 28, 2015), available at www.irs.gov/pub/irs-utl/lca-pia.pdf.
- ⁴² William J. Hunter & Michael A. Nelson, *An IRS Production Function*, 49 NAT’L TAX J. 105, 105–115 (Mar. 1996).
- ⁴³ IRS Publication 556, Examination of Returns, Appeal Rights, and Claims for Refund (Rev. Sept. 2013).
- ⁴⁴ *Id.*
- ⁴⁵ Department of Treasury, Internal Revenue Service, Request for Information Regarding *Advanced Analytics, Artificial Intelligence and Machine Learning Capabilities for the Cybersecurity Cloud Solution Program* (June 27, 2018), available at www.fbo.gov/index.php?s=opportunity&mode=form&tab=core&id=9e4ff975a1edb741ced23ed01c8512d&_cview=0.
- ⁴⁶ Department of Treasury, *Advanced Analytics, Artificial Intelligence and Machine Learning Capabilities for the Cybersecurity Cloud Solution Program* (revised Dec. 4, 2018), available at www.fbo.gov/index.php?s=opportunity&mode=form&tab=core&id=d5df279d2729d1c5b70d71b1b8c3dbf3&_cview=0.
- ⁴⁷ Department of Treasury, Internal Revenue Service, Request for Information Regarding Social Media Research Request (Dec. 18, 2018, modified Jan. 30, 2019, and Feb. 19, 2019), available at www.fbo.gov/index.php?s=opportunity&mode=form&tab=core&id=64bdd59ead1bf0df0eb9e5e42b85b89&_cview=0.
- ⁴⁸ *Id.*
- ⁴⁹ *Id.*
- ⁵⁰ See Code Sec. 6103(b)(2). FOIA does not apply to matters specifically exempted by another statute, which in this case is Code Sec. 6103. Attempts by taxpayers seeking information related to how DIF scores are calculated were unsuccessful. See *Gillin*, CA-1, 980 F.2d 819, 822 (1992) (“The IRS closely guards information concerning its DIF scoring methodology because knowledge of the technique would enable an unscrupulous taxpayer to manipulate his return to obtain a lower DIF score and reduce the probability of an audit.”); *Lamb*, DC-MI, 871 F.Supp 301 (1994) (holding that the IRS properly withheld records regarding DIF scores).

This article is reprinted with the publisher's permission from the Journal of Tax Practice & Procedure, a bi-monthly journal published by Wolters Kluwer. Copying or distribution without the publisher's permission is prohibited. To subscribe to the Journal of Tax Practice & Procedure or other Wolters Kluwer Journals please call 1-800-344-3734 or visit taxna.wolterskluwer.com. All views expressed in the articles and columns are those of the author and not necessarily those of Wolters Kluwer or any other person.



Wolters Kluwer