IN THE SUPREME COURT OF THE STATE OF CONNECTICUT

S.C. 20600

STATE OF CONNECTICUT,

v.

ONAJE SMITH

Amicus Curiae Brief of Upturn Inc., in Support of Defendant-Appellant

---

Jim Davy
PA I.D. No. 321631
All Rise Trial & Appellate
P.O. Box 15216
Philadelphia, PA 19125

Marisol Orihuela, Juris No. 439460
Jerome N. Frank Legal Services Org.
P.O. Box 209090
New Haven, CT 06520

Counsel for Amicus Curiae

DATE FILED: April 26, 2022

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

OTHER AUTHORITIES

STATEMENT OF INTEREST OF AMICUS CURIAE[1]

Upturn is a nonprofit organization based in Washington, D.C. that works with many leading civil rights organizations to advance equity and justice in the design, governance, and use of technology. One of Upturn's priorities is to ensure that technology does not exacerbate or entrench mass incarceration and racial inequity in the criminal legal system.

Upturn recently published *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones*. This report is the most comprehensive examination of law enforcement's use of mobile device forensic tools to date. Based on more than 110 public records requests, more than 12,000 pages of documents, and more than two years of research, the report documents the widespread proliferation and use of this technology by state and local law enforcement agencies.[2] Among the report's findings, more than 2,000 agencies have purchased these tools in all 50 states and the District of Columbia. State and local law enforcement agencies have performed hundreds of thousands of cellphone extractions since 2015, often without a warrant. Few departments have meaningful policies governing use of this technology. The report also documents the existing technical capabilities of today's mobile device forensic tools, finding that the tools provide sweeping access to personal information on a phone.[3]

---

[1] No portion of this brief was written by counsel for a party to this appeal. Neither any party to this appeal, nor its counsel, contributed to the cost of the preparation or submission of this brief. No person or entity, other than the amicus and its members, contributed to the cost of the preparation or submission of this brief.

[2] Every document *Amicus* received in response to these public records requests is publicly available. Those documents are available here: https://www.documentcloud.org/app?q=project%3Adevice-search-200411%20&page=1.

[3] To assess the technical capabilities of current mobile device forensic tools, *Amicus* extensively reviewed and examined technical manuals, software release notes, marketing materials, webinars, and digital forensics blog posts and forums. *Amicus* also consulted with one of the few public defenders in the U.S. with these forensic tools and staff in-house.

This Brief aims to aid the Court in its understanding of how mobile device forensic tools work and how mobile device forensic tools can be used to narrow a cellphone search. This Brief also argues that the Court should use its supervisory authority to craft rules for the issuance and execution of cellphone search warrants.

ARGUMENT

I. HOW MOBILE DEVICE FORENSIC TOOLS ENABLE LAW ENFORCEMENT TO SEARCH CELLPHONES

Every day, law enforcement agencies across the country search hundreds to thousands of cellphones. To search these phones, law enforcement relies upon mobile device forensic tools (MDFTs). An MDFT is a computer program and its hardware that can copy and analyze data from a cellphone. MDFTs enable law enforcement to both extract and analyze data. MDFT software can run on a regular desktop computer, on a dedicated device like a tablet, or on a "kiosk" computer. These tools are sold by a range of companies, including AccessData, Cellebrite, Grayshift, Magnet Forensics, MSAB, and OpenText.[4]

[4] This Court deserves more context on Grayshift's amicus brief. During Upturn's research on MDFTs, Upturn sued the New York Police Department ("NYPD") under New York's Freedom of Information Law. At NYPD's request, Grayshift filed a letter in that case asking the NYPD to "include it in their opposition to Upturn's petition." *See Upturn, Inc. v. N.Y.C. Police Dep't*, Index No. 162380/2019 N.Y. Sup. Ct. NYSCEF DOC. No. 28. https://iapps.courts.state.ny.us/nyscef/ViewDocument?docIndex=dguHgSLyBI6BIQuqX0Marw==. That letter, which was filed for the purpose of preventing Upturn from learning how law enforcement like the NYPD uses GrayKey, asserted that "the broad contours of how [GrayKey] works are not known outside of Grayshift," "Grayshift does not publicly comment on or otherwise publicly discuss Gray[K]ey *[sic]*," and "Grayshift stands to suffer irreparable commercial harm if *even seemingly innocuous commercial or technical information is released*" (emphasis added). Further, GrayKey is only available to law enforcement agencies — even if defense attorneys in Connecticut had the resources to do so, they would be unable to purchase this tool, even if just to understand how it works. This Court should treat Grayshift's claims appropriately. *See Upturn, Inc. v. N.Y.C. Police Dep't,* 2021 N.Y. Slip Op. 31129 (N.Y. Sup. Ct. 2021).

Investigators initiate the extraction process by plugging a phone into the computer or tablet. Cellebrite software, which is like other tools,[5] will then prompt the investigator to choose the kind of extraction to be performed and, sometimes, the categories and time range of data to extract.[6] Often, to extract data, tools may bypass a phone's security features by taking advantage of security flaws or built-in diagnostic or development tools.

There are a few methods for copying data from phones.

"Manual extraction" refers to when an investigator views a phone's contents like a normal user of the phone. Typically, investigators will take photographs or screenshots of the screen or videotape their exploration of a phone's content.

"Logical extraction" automates what can be done through manual extraction. In other words, it automatically extracts data that's presented on the phone to the user, using the device's application programming interface (API).[7] By way of analogy, a logical extraction is like ordering food from a restaurant: what you can get is limited to menu items, and the waitstaff (the API) oversees their delivery and organization.

"File system extraction" is like a logical extraction, but also copies other data, such as files or information in internal databases that a phone doesn't typically display to users. Continuing the restaurant analogy, this is akin to asking the chef for specific dishes that are not on the menu, which is possible at some restaurants, but not others.

---

[5] Typically, the tools either detect what kind of phone has been connected, or otherwise allow law enforcement to look up the kind of phone by its brand or model number.

[6] Pre-extraction display of the categories and time range of data is fact-specific, depending on phone make, model, operating system, settings, and the extraction type. This feature is often, but not always, available.

[7] 18F, "What are APIs? – Anecdotes and Metaphors," available at https://18f.github.io/API-All-the-X/pages/what_are_APIs-anecdotes_and_metaphors/ ("APIs are like the world's best retriever. You say, 'Fido - go fetch me X' and he brings you back X.").

"Physical extraction" refers to an extraction that copies data as it's physically stored on the phone's hardware — in other words, copying data bit-by-bit, instead of as distinct files. Data from a physical extraction must be restructured into files for anyone to make sense of it. A physical extraction is like going to a restaurant and sneaking into the kitchen to take the food (fully prepared menu items, ingredients, things in the trash) directly as it exists in the kitchen without mediation from the waitstaff.

After extraction, MDFT software programs allows law enforcement to efficiently analyze the data. MDFTs preserve information like filename and file location, but can also aggregate every file found into a searchable and filterable pool. For example, law enforcement can sort data by the time and date of its creation, by location, by file or media type, or by source application.[8] This means law enforcement can take data extracted from different apps on a phone and view them together as a chronological series of events. It also means they can view all pictures or videos from the phone in one place, as a grid of thumbnails, regardless of how they are organized or named on the phone.[9] MDFTs can also search for key terms across the entire phone (just as you might use Google to search the web), and display information about the results and where they're organized within the phone's file system.

II. MOBILE DEVICE FORENSIC TOOLS CAN BE USED TO NARROW THE SEARCH. BUT A TECHNICAL POSSIBILITY MEANS LITTLE WITHOUT THE FORCE OF LAW.

[8] This is possible because all files contain metadata including their date of creation, and dates of most recent access and modification.

[9] When you take a photo with your cellphone's camera application, the photo is stored in a different folder than photos taken using other applications, like Instagram or WhatsApp. With direct access to the phone's file system, someone may have to manually navigate in and out of levels of folders to find all of the images on a phone. But because images have predictable file extensions, MDFTs like Cellebrite's UFED can automate the process of looking for image files on the phone and aggregate them in one place.

At each stage of the mobile device forensic process there are opportunities to narrow the search. MDFTs can limit what information is *copied* from the phone or can limit what information will be *analyzed*. MDFT software has built-in pre- and post-extraction filtering and categorization features, all of which can help narrow the search of a cellphone.

The simplest MDFT feature that can be used to narrow the search is the logical extraction interface. Cellebrite software, at the beginning of a logical extraction, prompts users to select the general categories of data to extract from the phone. This takes place before any data is copied from the phone. These categories include "call logs," "photos," "contacts," and "SMS test messages." Data is then copied from the cellphone according to whether it fits one of the selected categories, based on its file type and/or location in the file system of the phone, or using the phone's own API. For example, law enforcement could limit a logical extraction to only text messages between March 1 and March 15.[10] These limits can be set *before* data is extracted by the MDFT, narrowing the range of data copied from the cellphone. This is because cellphones store data predictably under the two major operating systems (iOS and Android), and because all files contain integral metadata, such as each file's date of creation. Cellebrite tools also offer a "selective file system" extraction, which allows investigators to see which specific applications are present on the phone before extracting data. This method allows law enforcement to search for terms like "Facebook" or "Snapchat," or scroll through the list of available apps and then select them for extraction.

[10] Investigators do not need to see phone data in advance to set a tool like Cellebrite UFED to only select photos from a certain date range. With these filters, a MDFT will simply automatically inspect each file it finds on the phone, without the investigator seeing it, determine wither it fits into the filter, and only then copy the file. Files that don't fit the filter will not be copied over, so the investigator does not have to risk seeing them.

After extraction and during analysis, MDFTs offer comprehensive filtering and searching tools. Once the data is on the computer or tablet running the MDFT software, it can be more thoroughly sorted. Data can be sorted by its original location on the phone (*e.g.,* WhatsApp messages), or simply by media type (*e.g.,* photos). For example, Cellebrite software separates the various categories of data — like "SMS Messages," "Pictures," "Device Locations," or "Contacts," and data from individual apps — and allows investigators to view each category separately. In addition, investigators can use keywords to search (*e.g.,* "Jane Doe," "2025221234," or "janedoe@hotmail.com") across all data categories, or limit data displayed to only communications involving a certain phone number or contact over a certain period. More complex analytical features include the ability to view data with attached GPS information (like photos taken with the phone's camera) on a map, and use predictive analytics to assess whether certain data (like texts or photos) is "related" to certain predefined categories like "drugs," "weapons," or "nudity."

Regardless of the specific method, MDFTs make it possible to narrow the search. This means that an investigator does not need to access or review every file on a device to determine if it is relevant.

III. THIS COURT SHOULD NOT BE LED ASTRAY BY CLAIMS THAT BECAUSE DIGITAL EVIDENCE ON CELLPHONES MIGHT BE DISGUISED OR MANIPULATED, LAW ENFORCEMENT MUST BE EMPOWERED TO SEARCH THE ENTIRE CELLPHONE.

Law enforcement claim that because digital data on cellphones may be disguised or manipulated, they will not know where evidence will be located. As a result, they argue that they must be able to seize and search everything on a cellphone. This argument falls apart upon basic inspection.

First, this argument ignores how most modern cellphones store information and what information is accessible to cellphone users. While courts have frequently likened cellphones to computers, modern cellphones operate differently from computers "because mobile operatizing systems are designed for ease of use and do not emphasize user-directed file organization." Andrew D. Huynh, *What Comes After Get a Warrant: Balancing Particularity and Practicality in Mobile Device Search Warrants Post-Riley*, 101 Cornell L. Rev. 187, 207-208 (2015). "As any iPhone or Android user can tell, users no longer determine where an app stores its files, because users have no direct access to the file directory." Laurent Sacharoff, *The Fourth Amendment Inventory as a Check on Digital Searches*, 105 Iowa L. Rev. 1643, 1660 (2020). This layer of abstraction over the cellphone's core functions (that computers do not exhibit to the same extent) means that cellphone users are generally not able to directly manipulate their cellphone data.

Second, this argument ignores how MDFTs operate. MDFTs are agnostic toward file organization or file name. While a file's name or pathing may be useful for contextualizing data, MDFTs can simply traverse through all data on a phone and pick out data that has a particular data type, where file type is distinct from the name of a file (which most cellphone users do not control, anyway). As a result, even in the rare instance in which digital data may be disguised or manipulated, MDFTs can surface files based on their actual content, regardless of how a file is named or where it is located. This means that an image file hidden in an unexpected folder and renamed with a misleading file extension can still be discovered.

Third, this forces the exception to become the rule. Courts "have allowed the very rare prospect of the computer mastermind to drive the entire doctrine, rather than taking the most typical user as the prototype." *Id*., at 1658.

IV. CELLPHONE SEARCHES MERIT *SUI GENERIS* FOURTH AMENDMENT TREATMENT

A "cell phone search would typically expose the government to far more than the most exhaustive search of a house." *See Riley v. California*, 573 U.S. 373, 396 (2014). Combined with search warrants that are so broadly and ambiguously worded as to be limitless, MDFTs compound the issue: they facilitate exhaustive and indiscriminate searches of cellphones by law enforcement. *Amicus's* research demonstrates this happens hundreds of thousands of times per year, often in cases where the nexus between a cellphone's data and the alleged offense is tenuous. This arrangement is constitutionally untenable. More must be done, which is why cellphone searches merit *sui generis* treatment. *See* Cameron Cantrell, *A Dignitary Fourth Amendment Framework and Its Usefulness for Mobile Phone Searches*, 25 Va. J.L. & Tech 242 (2022). This Court should use its supervisory authority to craft specific guidance for the issuance and execution of cellphone search warrants. This guidance should clearly prescribe heightened particularity and overbreadth requirements for cellphone searches.

First, the Court's guidance should require that cellphone search warrants "specify the particular items of evidence to be searched for and seized from the phone and be strictly limited to the time period and information or other data for which probable cause has been properly established." *See Burns v. United States*, 235 A.3d 758, 773 (D.C. 2020). Rather than permitting

> law enforcement officers to operate through inferences, the Fourth Amendment demands a cellphone warrant specify the types of data to be seized with sufficient detail to distinguish material for which there is probable cause from information that should remain private. *See State v. Fairley* 457 P.3d 1150, 1154 (Wash. Ct. App. 2020).

To be sufficiently particular, "a warrant for a cell phone search presumptively must contain some temporal limit …. [and] should err on the side of narrowness." *See Commonwealth v.*

Snow, 486 Mass. 582, 594, 160 N.E.3d 277, 288 (2021). Further, the nexus between each category of information on a cellphone — such as texts, photographs, contacts, or emails — and the alleged criminal offense must be specific and clear. Cellphone search warrants to must be based on more than the fact that a defendant has a phone and the truism that people use phones to do seemingly everything. *See United States v. Opoku*, 556 F. Supp. 3d 633, 644 (S.D. Tex. 2021).

Second, the guidance should make clear that search warrants that authorize a search of "any and all cellphone data" or authorize a search of a laundry list of cellphone data are presumptively invalid. Catch-all provisions should be forbidden. The same is true of search warrants that authorize a search of a cellphone for "evidence related to this and other criminal offenses." Such warrants offer no limitations or restrictions on a search of a cellphone.

To illustrate, consider two hypotheticals. In Case A, a search warrant authorizes law enforcement to search a cellphone for "evidence of criminal threats that occurred over text message on January 15, 2021." In Case B, a search warrant authorizes law enforcement to search a cellphone for "evidence relating to possession of marijuana and/or distribution of marijuana." In Case A, it's highly likely that two different investigators will perform the same kind of search with an MDFT and return with similar evidence given the warrant's clear restrictions on the type of data and the timeframe. In Case B, one investigator might explore internet search history, calendar entries, text messages, dating app messages, and geolocation data amassed from apps downloaded onto the phone. Another might limit their search just to text messages and photos. Ultimately, it is unlikely they will perform the same search, or return with the same evidence. While one investigator may take reasonable steps

in their search, another might not, largely depending on how they exercise their unfettered discretion and where each investigator thinks they could find evidence.

Third, the guidance should not extend the plain view exception to cellphone search warrants. The plain view exception "may not be used to extend a general exploratory search … until something incriminating at last emerges." *See Coolidge v. New Hampshire* 406 U.S. 443, 466 (1971). But in digital searches nearly anything can come into plain view. This "undercuts the plain view's pivotal assumption" — that any intrusion would be "minor" — and "effectively converts the plain view doctrine into a vehicle for the execution of a general warrant." *See State v. Bock*, 310 Or. App. 329, 339, 485 P.3d 931, 938 (2021).

Fourth, cellphone search warrants cannot rely on general statements that digital data may be disguised or manipulated to justify a search of the entire phone. If law enforcement has specific evidence to believe a more technically sophisticated user took steps to conceal digital data on a cellphone, they can seek a broader warrant based on that specific evidence.

Finally, the guidance should insist upon the production of digital audit logs created by the MDFT upon return of the warrant. Such logs would document the precise steps that law enforcement took when searching a phone to ensure compliance with the warrant. In particular, audit logs could equip judges to assess the reasonableness of a search technique and ascertain if the search was sufficiently tailored to the search warrant.

V. CONCLUSION

Every day across the country, hundreds to thousands of cellphone searches occur. Without guidance from this Court clearly establishing heightened requirements for cellphone search warrants, mobile device forensic tools will continue to facilitate indiscriminate searches of cellphones that sit at odds with the Fourth Amendment's protections.

Respectfully submitted,

/s/ Jim Davy
Jim Davy
PA I.D. No. 321631
All Rise Trial & Appellate
P.O. Box 15216
Philadelphia, PA 19125

/s/ Marisol Orihuela
Marisol Orihuela
Jerome N. Frank Legal Services Org.
All Rise Trial & Appellate
P.O. Box 209090
New Haven, CT 06520

Counsel for *Amicus Curiae* Upturn

April 26, 2022

CERTIFICATION

Pursuant to Practice Book § 62-7, on this 26th day of April, 2022, the undersigned hereby certifies that this document complies with all format provisions and further certifies that a copy of the foregoing was delivered in-hand, by first-class mail, postage pre-paid, or by fax or electronic delivery to:

Jennifer Smith
Assistant Public Defender
Office of the Chief Public Defender
Legal Services Unit
55 W. Main Street, Suite 430
Waterbury, CT 06702
Email: Jennifer.Smith@pds.ct.gov
Tel. (203) 574-0029

Ronald G. Weller
Senior Assistant State's Attorney
Office of the Chief State's Attorney
Appellate Bureau
300 Corporate Place
Rocky Hill, CT 06067
Email: Ronald.Weller@ct.gov, DCJ.OCSA.Appellate@ct.gov
Tel. (860) 258-5807

Thadius L. Bochain
Deputy Assistant State's Attorney
Office of the Chief State's Attorney
Appellate Bureau
300 Corporate Place
Rocky Hill, CT 06067
Thadius.Bochain@ct.gov, DCJ.OCSA.Appellate@ct.gov
Tel. (860) 258-5807

/s/ Marisol Orihuela
Marisol Orihuela

CERTIFICATION

The undersigned attorney hereby certifies, pursuant to Connecticut Rules of Appellate Procedure § 67-2, that:

(1) the electronically submitted brief has been delivered electronically to the last known e-mail addresses of each counsel of record for whom an email address has been provided; and

(2) the electronically submitted brief and the filed paper brief and appendix have been redacted or do not contain any names or other personal identifying information that is prohibited from disclosure by rule, statute, court order or case law; and

(3) a copy of the brief has been sent to each counsel of record and to any trial judge who rendered a decision that is the subject matter of the appeal, in compliance with § 62-7; and

(4) the brief being filed with the appellate clerk are true copies of the brief that was submitted electronically; and

(5) the brief complies with all provisions of this rule.

/s/ Marisol Orihuela
Marisol Orihuela

Counsel for Amicus

256 F.Supp.3d 355
United States District Court, S.D. New York.

UNITED STATES of America,

v.

Benjamin WEY, Defendant.

15–CR–611 (AJN)
|
Filed 06/13/2017
|
Signed June 14, 2017

Synopsis

Background: Defendant was charged with securities and wire fraud, as well as money laundering. Defendant moved to suppress.

Holdings: The District Court, Alison J. Nathan, J., held that:

warrants to search defendant's business and apartment failed to identify suspected crimes;

warrants set forth expansive categories of generic items subject to seizure without linking to suspected criminal activity;

warrants lacked temporal limitation;

all records exception did not apply;

warrants were overbroad; and

good faith exception to exclusionary rule did not apply.

Motion granted.

Attorneys and Law Firms

***359** Andrew Caldwell Adams, Brooke Elizabeth Cucinella, Ian Patrick McGinley, Michael Ferrara, Sarah Kathleen Eddy, Brendan Francis Quigley, United States Attorney's Office, New York, NY, for United States of America.

Barry McNeil, Haynes and Boone, LLP, Dallas, TX, Joseph Craig Lawlor, Sarah Elizabeth Jacobson, David Mark Siegal, Haynes and Boone, LLP, New York, NY, for Defendant.

OPINION & ORDER [CORRECTED]

ALISON J. NATHAN, District Judge:

Defendant Benjamin Wey faces an eight-count indictment charging him with securities fraud, wire fraud, conspiracy to commit securities and wire fraud, money laundering, and failure to disclose beneficial ownership of publicly traded companies. Before the Court is Wey's motion to suppress evidence seized during Government searches of his residence and the offices of his consulting firm, New York Global Group, Inc., both conducted on January 25, 2012. For the reasons set forth below, Wey's motion is GRANTED.

I. Background

A. The Indictment

Wey is charged in an eight-count indictment returned on September 8, 2015. Dkt. No. 2 (the "Indictment"). The Indictment alleges that between approximately 2007 and 2011, Wey, along with co-Defendant Seref Dogan Erbek (who remains at large) and unindicted co-conspirators known and unknown, orchestrated a scheme whereby Wey—through various non-party entities, family members, and associates (the "Nominees")—covertly amassed beneficial ownership of substantial portions of the equity stock of certain publicly traded companies (the "Issuers"), manipulated the market price of the Issuers' stock, liquidated his holdings at artificially inflated prices, and then laundered millions of dollars in ill-gotten proceeds. *See, e.g.,* Indictment ¶¶ 7, 13, 18–22.

Specifically, according to the Indictment, Wey secretly caused the Nominees to acquire, on his behalf, substantial portions of the shares of certain U.S.-based over-the-counter-traded shell companies and then, ***360** through his consulting firm New York Global Group, Inc. ("NYGG") and its alleged affiliate in Beijing, China, facilitated so-called "reverse merger" transactions by which China-based operating companies merged into those shell companies, thus forming new publicly traded corporations—the Issuers. *Id.* ¶¶ 8–12. The Government alleges that the Nominees acquired and retained, for Wey's benefit, stock in the Issuers

by virtue of their ownership of the target shell companies, and that these holdings together constituted more than five percent of the Issuers' outstanding shares. *Id.* ¶¶ 7, 13. Because Wey, among other things, purportedly exercised investment authority over the shares held by the Nominees, he was required to disclose his beneficial ownership under Section 13(d) of the Securities Exchange Act of 1934 and Rule 13d–1 promulgated thereunder within ten days of the acquisition of shares in excess of five percent. *Id.* ¶ 13. The Government alleges that Wey was "well aware" of this reporting requirement but intentionally failed to file the required disclosures in order to conceal his ownership from the investing public. *Id.* ¶ 14.

Wey also, according to the Indictment, caused several of the Issuers, including SmartHeat, Inc. ("SmartHeat"), Deer Consumer Products, Inc. ("Deer"), and Clean Tech Innovations, Inc. ("CleanTech"), to apply for listings on the Nasdaq. *Id.* ¶ 15. In order to secure approval of these applications, Wey allegedly engaged in deception to artificially satisfy Nasdaq's so-called "round-lot" shareholder requirement—i.e., the requirement that every listed issuer has at least 300 shareholders each owning 100 or more shares of common stock. *Id.* ¶¶ 16–17. In particular, Wey purportedly facilitated deceptive transfers of shares of Issuer stock from Nominees to other Wey confederates, as well as issuances of round-lot blocks of shares in the names of individuals who never actually received such shares or were otherwise unaware of their ownership. *Id.* ¶¶ 15–17.

After successfully getting the Issuers listed on Nasdaq, the Government alleges, Wey proceeded to manipulate the demand for and price of Issuer stock. This was purportedly accomplished by, among other things: (i) causing Manhattan-based retail brokers to solicit their customers to purchase common stock of the Issuers, often on margin, while at the same time actively discouraging the sale of such stock; (ii) instructing Erbek to maintain the share prices of certain Issuers' stock held in various Nominees' accounts; and (iii) facilitating match trades in the Issuers' stock involving Nominees and/or other Wey confederates. *Id.* ¶¶ 18–19.

Contemporaneous with this market manipulation scheme, the Government alleges, Wey caused certain Nominees to sell shares of the Issuers' stock at artificially inflated prices. *Id.* ¶ 20. Wey then purportedly laundered the proceeds of these sales by causing them to be transferred from accounts located in the U.S. to Nominees' accounts located overseas, including in Switzerland and Hong Kong, before being repatriated back to the U.S. and into accounts controlled by Wey and his wife or otherwise held for Wey's benefit. *Id.* ¶¶ 20–22.

Wey is charged with one count of conspiracy to commit securities fraud and wire fraud under 18 U.S.C. § 371; one count of securities fraud under Section 10(b) of the Exchange Act and Rule 10b–5 promulgated thereunder, 15 U.S.C. §§ 78j(b) & 78ff, 17 C.F.R. § 240.10b–5; one count of securities fraud under 18 U.S.C. § 1348; one count of wire fraud under 18 U.S.C. § 1343 ("Count Four"); two counts —concerning Deer and CleanTech stock, respectively—of failure to disclose ***361** ownership in excess of five percent of a covered class of equity securities under Section 13(d) of the Exchange Act and Rule 13d–l, 15 U.S.C. §§ 78m(d) & 78ff, 17 C.F.R. § 240.13d–l; one count of money laundering under 18 U.S.C. § 1956(a)(l)(B)(i); and one count of money laundering under 18 U.S.C. § 1956(a)(2)(A). *See* Indictment ¶¶ 23–40.

B. The Search Warrant Affidavits

1. Affidavit Concerning NYGG's Offices

On January 24, 2012, Special Agent Matthew F. Komar of the Federal Bureau of Investigation ("FBI") swore out an affidavit in support of an application for a warrant to search NYGG's Manhattan offices located at 40 Wall Street, Suite 3800. *See* July 8, 2016 Declaration of Matthew F. Komar Ex. 1, Dkt. No. 54–1 (the "Komar Affidavit" or "Komar Aff."). The Komar Affidavit described an ongoing FBI investigation of Wey, Wey's sister (a Chinese citizen apparently employed by NYGG or its purported Beijing-based counterpart), and NYGG itself—which it characterized as a "corporate advisory firm" founded by Wey in approximately 2004 that specialized in "introducing middle-market Chinese operating companies to the U.S. capital markets." *See, e.g.,* Komar Aff. ¶¶ 2–7, 16. It asserted that there was probable cause to believe that fruits, instrumentalities, and evidence of violations of the federal securities, mail, and wire fraud laws were located within the subject premises. *See, e.g., id.* ¶¶ 2–7.

Based on the investigation to date, including information obtained from current and former NYGG employees, the Komar Affidavit detailed a suspected "fraud and market manipulation scheme" perpetuated by Wey, acting through NYGG and other entities. *See, e.g., Id.* ¶¶ 4–14. Komar's description of the purported scheme broadly tracked, in substantial measure, the allegations set forth in the

Indictment and discussed above. As outlined in the Komar Affidavit, the scheme involved Wey retaining undisclosed beneficial ownership of Issuers created through reverse merger transactions facilitated by NYGG and then artificially inflating the Issuers' round-lot shareholder bases to secure Nasdaq listings and manipulating demand for the Issuers' stock by encouraging a "a hand-picked team of retail stock brokers" to "aggressively solicit purchases" of the Issuers' securities. Wey would then, according to the Affidavit, effectuate the sale of Nominee-held shares at inflated prices and launder the proceeds, including through fund transfers to Wey's wife. *See, e.g., id.* ¶¶ 8–14, 18–29.

Notwithstanding its length, the Komar Affidavit is notable for its focus on Wey's connection to a handful of specific companies. Like the Indictment, the Komar Affidavit principally addressed SmartHeat, Deer, and CleanTech. *Id.* ¶¶ 11–12, 18–20, 35–36. With respect to SmartHeat and Deer, the Affidavit discussed particular purported misrepresentations made by the Issuers, and by Wey, to Nasdaq in the course of the listing application process and described serial transactions by which Wey allegedly inflated the Issuers' round-lot shareholder bases in 2008 and 2009. *Id.* ¶¶ 18–19. It further set out alleged market manipulation tactics undertaken in 2009 through 2010 by the broker group over which Wey purportedly exercised influence, including improper high-pressure promotion of Issuer securities and misrepresentations concerning the future value of the stocks. *Id.* ¶¶ 20–25. A $350,000 kickback allegedly paid to the broker group in connection with its promotion of Deer, at least, was described in some detail. *Id.* ¶ 26. The Affidavit also discussed, to some extent on a transaction-level basis, the ***362** Nominees' sales, in 2009 and 2010, of large blocks of Issuer shares at purportedly inflated prices and the wiring of the sale proceeds to accounts linked to Wey confederates and family members in Switzerland and Hong Kong and, ultimately, back to the U.S. *Id.* ¶¶ 27–29.

As to CleanTech, the Affidavit described Wey's purported facilitation in 2010 and 2011 of the placement of Issuer stock with individuals and entities formerly used as Nominees with respect to Deer and SmartHeat. *Id.* ¶ 36. It also identified documents allegedly demonstrating Wey's indirect control over CleanTech, and discussed Nasdaq's decision to delist CleanTech based on its alleged failure to disclose materials revealing its financial connection to Wey.[1] *Id.* The Affidavit further recounted information from an FBI source within NYGG suggesting that Wey facilitated CleanTech management's preparation of inflated revenue forecasts, and identified a pattern of active trading in CleanTech stock by Wey's alleged retail broker team. *Id.*

Of note, the Komar Affidavit also identified by name dozens of individuals and entities potentially involved, directly or indirectly, in Wey's suspected schemes. These included, among others, the U.S.-based broker-dealer team purportedly working at Wey's direction and several firms at which its members were employed, senior employees of the Issuers, suspected Nominees and other Wey associates and family members in both the United States and China, and NYGG personnel. *Id.* ¶¶ 12, 14, 18–19, 24, 26–29, 33, 36.

The Affidavit also connected Wey, more briefly, to several other specific companies of evident interest to the Government. It described, for example, Wey's and NYGG's facilitation of a reverse merger transaction involving Bodisen Biotech, Inc., as well as that company's subsequent delisting by the then-American Stock Exchange for, among other things, failure to properly disclose its relationship with and payments to NYGG. *Id.* ¶ 17. It also recounted Wey's alleged involvement in an accounting fraud scheme perpetuated by AgFeed Industries, Inc., a publicly-traded company born of another reverse merger transaction purportedly facilitated by Wey, and large-scale sales of AgFeed stock by investors believed to be Wey Nominees. *Id.* ¶¶ 30–34. Finally, the Affidavit asserted that Wey exercised undisclosed control over Nova Lifestyle, Inc. (yet another product of a Wey-linked reverse merger transaction), that he wielded that control to effectuate share transfers to Nominees, and that he directed NYGG employees to improperly solicit purchases of the company's stock. *Id.* ¶ 37.

In addition, the Komar Affidavit included a short section devoted to Wey's personal background and alleged history of participating in fraudulent activities, including within the securities industry. It asserted, among other things, that Wey was sanctioned by both the Oklahoma Department of Securities and then-National Association of Securities Dealers based on misconduct during Wey's time working as a registered investment adviser in Oklahoma in the mid to late 1990s and early 2000s. It further averred that Wey engaged in various forms of tax and other financial fraud and forgery during roughly the same period. *Id.* ¶ 15.

Based on these submissions, and as discussed further below, the Komar Affidavit formally requested permission to seize from NYGG's offices twelve expansive ***363** categories of materials set forth on an appended exhibit, with the limitation

that the materials concern at least one of an independently appended list of approximately 220 named individuals and entities believed to be in some way connected to Wey's purported scheme. *Id.* ¶¶ 35, 38–42, 46–47, Exs. A–B. It also sought court approval to seize, copy, and/or digitally image computers and related electronic equipment believed to contain such materials and to conduct offsite searches of the devices' contents. According to the Komar Affidavit, in view of the highly technical and specialized procedures and substantial time investment required to effect thorough searches of the potentially voluminous data contained within this equipment—including deleted, concealed, or encrypted files—and extract relevant material while maintaining the integrity of the evidence, it would in many cases be impractical, if not impossible, to effectively do so onsite. *Id.* ¶¶ 43–47, Ex. C. As such, the Affidavit attached a third exhibit setting forth a proposed methodology for reviewing and seizing such equipment and, if necessary, executing offsite searches. *Id.* Ex. C.

2. Affidavit Concerning Wey's Residence

As discussed further below, during the course of the Government's search of the NYGG offices the following day, it decided to apply for a warrant to search the Manhattan apartment that Wey shared with his wife, Michaela, and their children (the "Wey Apartment"). Accordingly, on January 25, 2012, Special Agent Keith Garwood of the FBI swore out another affidavit. *See* July 8, 2016 Declaration of Matthew F. Komar Ex. 4, Dkt. No. 54–4 (the "Garwood Affidavit" or "Garwood Aff"). The Garwood Affidavit—which relied heavily upon and expressly incorporated by reference the Komar Affidavit—explained that FBI personnel had interviewed NYGG employees during the search of the firm's offices earlier that day and learned that Michaela Wey served as NYGG's "office manager" and "bookkeeper" but generally worked out of the Wey Apartment, where she would, among other things, perform accounting and payroll functions and mail checks. Garwood Aff. ¶¶ 2, 7–11. It also cited assertions in the Komar Affidavit that Wey caused certain Issuer stock certificates for new round-lot shareholders to be sent to the Wey Apartment, that certain Nominees had wired substantial sums of money to accounts held in the name of Michaela Wey, and that Michaela Wey had once been listed in an SEC filing as an executive officer of NYGG. *Id.* ¶¶ 6, 9, 12.

Based on that information, the Garwood Affidavit urged that there was probable cause to believe that fruits, instrumentalities, and evidence of securities, mail, and wire fraud would be found within the Wey Apartment and sought permission to seize from the Apartment substantially the same categories of materials, pertaining to substantially the same individuals and entities, listed in the Komar Affidavit. Garwood Aff. ¶ 4, 13–16, 20, Exs. A–B. It also sought approval of substantially the same protocol as that proposed in the Komar Affidavit for searching computers and related equipment offsite, citing similar practicality concerns. *Id.* 17–20, Ex. C.

C. The Search Warrants

1. The NYGG Warrant

United States Magistrate Judge Michael H. Dolinger approved the Government's application with respect to the NYGG offices and issued a corresponding search warrant on January 24, 2012. *See* May 27, 2016 Declaration of David Siegal ("Siegal Dec.") Ex. 8, Dkt. No. 46–9 (the "NYGG Warrant"). The NYGG Warrant identified the premises to be searched as "[t]he office ***364** of [NYGG] at 40 Wall Street, 38th Floor, Suite 3800, New York, New York, and any closed or locked cabinets, briefcases, and other containers kept therein, including computers and electronic storage devices, excluding the individual office of James Baxter, Esq." *Id.* Ex. A.

The property to be seized pursuant to the NYGG Warrant was defined through the interplay between two attached exhibits (both of which had originally been included in the Government's application in substantially identical form). Specifically, Exhibit A to the NYGG Warrant set forth, by category, the types of materials subject to seizure along with illustrative lists, and imposed the additional requirement that the actual materials to be seized relate in some way to at least one of a list of individuals and entities included in Exhibit B. The scope of Exhibit A is best illustrated by reproducing it in full, with top-line categories emphasized relative to their non-exhaustive supporting lists, as applicable:

> 1. **Financial records concerning the individuals and entities listed in Exhibit B** ... including banking and brokerage firm account statements, checks, and transactions records, wire transfer instructions and similar documents concerning or reflecting movements of funds,

account and account holder information, check numbers, account numbers and Federal Reserve routing numbers;

2. **Personal financial records of any individuals named in Exhibit B or of any employees, agents, or shareholders of any of the entities listed in Exhibit B,** including banking and brokerage firm account statements, checks, and transaction records, wire transfer instructions and similar documents concerning or reflecting movements of funds, account and account holder information, check numbers, account numbers and Federal Reserve routing numbers;

3. **Telephone bills, telephone message pads, notes, memoranda and other records of internal and external communications between, among, or relating to any of the individuals and entities listed in Exhibit B;**

4. **Correspondence, audio tapes, and video tapes concerning any of the individuals and entities listed in Exhibit B;**

5. **Hotel, airline and credit card receipts reflecting the dates and locations of meetings or travel to meetings concerning any of the individuals and entities listed in Exhibit B;**

6. **Photographs, address books, Rolodexes, diaries, income tax returns and calendars concerning the operations and management of any of the individuals and entities listed in Exhibit B;**

7. **Computers, flash drives, internal and external hard drives, diskettes and other magnetic storage media, and files, data and information contained thereon, used to store names, telephone numbers and addresses, and other information,** including but not limited to personal digital assistants such as iPhones, iPads, Blackberrys, smartphones, and cellphones, as well as drafts and final versions of documents and correspondence, used by, or used in connection with the individuals and entities listed in Exhibit B....;

8. **Marketing materials relating to any of the individuals and entities listed in Exhibit B,** including offering materials, private placement memoranda, sales scripts, investor "lead" lists, investment agreements, financial statements, and other documents concerning, ***365** [or] relating to, the purchase or sale of securities;

9. **Documents identifying shareholders or investors in the entities listed in Exhibit B,** including transfer agent records, stock certificates, investor lists, investor files, investment subscription agreements, copies of checks received from or sent to investors, copies of account statements sent to investors, copies of correspondence sent to or received from investors, Federal Express, DHL or other records reflecting mailings by private commercial carriers and the U.S. Postal Service, and other documents concerning or reflecting the identities and participation of investors in such schemes;

10. **Documents reflecting the ownership by the individuals and entities listed in Exhibit B of real properties and personal property purchased with the proceeds of fraud,** including but not limited to houses, apartments, cars, boats, and jewelry, including purchase and sale agreements, deeds, mortgage documents, and other real estate or other property closing documents;

11. **Identification documents and other documents which may reflect the identities of persons listed in Exhibit B or persons affiliated with the entities listed in Exhibit B**; and

12. **Corporate documents reflecting the ownership or structure of, or relationship between and among, any of the entities listed in Exhibit B,** including incorporation documents, inter-company agreements, lists of partners and stockholders, organizational charts, and corporate resolutions and bylaws.

NYGG Warrant Ex. A.

Exhibit B to the NYGG Warrant, in turn, named the same approximately 220 individuals and entities identified in Exhibit B to the Komar Affidavit. Of great significance, the list included among its first two entries NYGG itself (whose offices, of course, would be the subject of the search) and Wey himself. *See* NYGG Warrant Ex. B. Reading Exhibits A and B together, then, the NYGG Warrant authorized the seizure from NYGG's offices of, for example, all "financial records," "internal and external communications," "correspondence," and other things concerning NYGG.

Beyond the requirement that the materials subject to seizure relate to at least one of the Exhibit B individuals/entities, the NYGG Warrant imposed no substantive limitations. It did not specify the crimes under investigation, whether by statutory citation or otherwise, or discuss any particular conduct of

interest. It did not set out any date ranges or other timeframe-based criteria. Importantly, the NYGG Warrant also did not attach, incorporate, or otherwise expressly reference the Komar Affidavit.

With respect to any "computers, computer-related equipment, and other electronic devices" found on the premises, the NYGG Warrant provided that the FBI would employ substantially the same search and seizure methodology proposed in the Komar Affidavit, which it described in another attached Exhibit (essentially, a copy of Exhibit C to the Komar Affidavit). *See* NYGG Warrant Exs. A, C. That methodology contemplated, in sum and substance, that FBI personnel trained in searching and seizing computer data would conduct an initial onsite review of any such items. *Id.* Ex. C. If a determination were made that a given item could not be searched onsite "within a reasonable amount of time and without jeopardizing the ability to preserve data," then the FBI could either (i) copy its data for offsite review (if the device were found not to contain contraband) or (ii) seize the device ***366** for transportation to a law enforcement laboratory for offsite review (if the device were found to contain contraband or onsite data review or copying would be impractical). *Id.* In searching these items or their copies, the FBI would be permitted "to examine all of the data contained" but only "to view their precise contents and determine whether the data falls within the items to be seized as set forth" elsewhere in NYGG Warrant. *Id.* In other words, the procedures for searching computer equipment and electronic devices did not purport to expand or restrict the scope of the materials subject to seizure; rather, data from these items could ultimately be seized only if it fell within the "strictures"—such as they were—of Warrant Exhibits A and B. During these searches, the FBI would be required to "have procedures in place to segregate any potentially privileged materials or files." *Id.* If it were determined that any confiscated devices were "no longer necessary to retrieve and preserve the data" and that the "items [were] not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(b)," the Government would be required to "return these items, upon request, within a reasonable period of time." *Id.*

2. The Wey Apartment Warrant

Magistrate Judge Dolinger also approved the Government's application to search the Wey Apartment, issuing a warrant on January 25, 2012 (during the course of the Government's search of the NYGG offices, as discussed further below). *See* Siegal Dec. Ex. 24, Dkt. No. 46–25 (the "Apartment Warrant"). Other than its description of the premises to be searched, the Apartment Warrant was substantially identical in all material respects to the NYGG Warrant, right down to its incorporation of copies of the same three Exhibits. *Id.* & Exs. A–C. Of particular note in the context of the forthcoming search of the Wey Apartment, Exhibit B (the list of relevant individuals and entities) included not only Wey himself but also Michaela Wey. Thus, the Apartment Warrant authorized the seizure from the Wey Apartment of, for example, all "financial records," "internal and external communications," "correspondence," "photographs," "audio tapes," and "video tapes" concerning either of the Apartment's two adult occupants.

D. The Searches

After Wey filed the instant suppression motion, the Court made a preliminary determination that a hearing was warranted to address whether the Government acted in good faith in executing the NYGG Warrant and the Apartment Warrant and whether the Government acted reasonably and in good faith in executing off-site searches of computers and computer-related equipment recovered during the execution of the Warrants. Dkt. No. 69. Accordingly, the Court conducted a two-day suppression hearing on January 23 and January 24, 2017 (the "Hearing"), at which it heard live testimony from former Assistant United States Attorney David Massey, Special Agent Komar, Special Agent Thomas McGuire, Special Agent Elizabeth Miller, forensic examiner and information technology specialist Brian Booth.[2]

What follows for the remainder of this Opinion constitutes the Court's findings of fact and conclusions of law. They are based upon the evidence taken at the hearing—with ***367** the benefit of supplemental post-hearing briefing and oral argument—as well additional evidentiary submissions by the parties in support of their original and supplemental briefs.

1. Preparation for the NYGG Search

The Government's investigation into Wey and NYGG was already at least several months old when the Government applied for the NYGG Warrant on January 24, 2012. Hearing Tr. 30:11–14. The investigation was led, during that period of time, by Agent Komar and then-AUSA David Massey. Hearing Tr. 14:16–20, 29:9–12, 120:11–15. AUSA Massey testified that the decision to apply for the NYGG Warrant was

made "at least" several weeks—and "perhaps" even months—before the Government submitted its application. *Id.* at 30:23–31:4.

In preparation for the Government's search of the NYGG offices, Agent Komar prepared an "operations order form" for circulation to the FBI search team (the "Operations Order"), which was comprised of approximately twenty agents predominantly from the C–43 securities fraud squad and/or the Computer Analysis Response Team ("CART"), along with personnel from the FBI's photography unit. Hearing Tr. 119:21–120:2, 122:10–123:16, 185:18–186:5, 236:22–237:4; Gov't Exs. 1 (Operations Order), 5 (FBI Crime Scene Sign–In Log for Search of NYGG). The Operations Order contained a "synopsis of the case," authored by Komar, which asserted that there was probable cause to believe that Wey, acting through NYGG, had "committed securities fraud and manipulated the market for the securities of various small-capitalization issuers." Hearing Tr. 122:25–123:4; Gov't Ex. 1 at 1. The Operations Order then proceeded to outline in a brief paragraph the basic contours of the suspected scheme, substantially consistent with the Komar Affidavit:

> Wey introduces Chinese companies to the U.S. markets and arranges reverse mergers and assists these companies [in] get[ting] listed on markets such as Nasdaq. It appears he has artificially inflated the number of round-lot shareholders for the purpose of meeting listing requirements. Wey then retains undisclosed beneficial ownership and/or control of large blocks of shares of the Chinese companies that are held in the name of nominees. Wey creates an artificial demand for the securities by working directly with a hand-picked team of retail stock brokers ... to aggressively solicit purchases of the Chinese companies' securities. Once the artificial demand is created and the stock price goes up, Wey sells the large block of nominee held shares.

Id. In a separate section, the Operations Order described the forthcoming operation as a search "for documents related to Wey assisting Chinese reverse mergers [to] falsify their records to meet listing standards for Nasdaq" and "control[ing] the trading volume in these Chinese companies, through a number of associated broker dealers." *Id.* at 5. The Operations Order did not reference or name any of the specific Issuers implicated in Wey's alleged scheme. Nor did it discuss any of the entities or individuals listed on Exhibit B to the NYGG Warrant (apart from NYGG and Wey) or explain their purported connections to the suspected criminal activities.

Late in the afternoon of January 24, 2012—the same day that the NYGG Warrant issued and the day before it was to be executed—Agent Komar and AUSA Massey conducted a pre-operation briefing attended by all members of the FBI search team. Hearing Tr. 15:6–16:3, 122:1–4, 123:19–124:–2. The briefing lasted approximately 45 minutes to an hour. *Id.* 240:24–25. ***368** During the briefing, AUSA Massey explained the nature of the scheme under investigation, using the Komar Affidavit as a reference, and described the "types of documents" that the team would be "looking for." *Id.* 68:25–71:17, 124:11–15; 239:7–21. Agent Komar summarized "some parts" of the investigation to date but primarily briefed the team on operational logistics for the coming search. *Id.* 124:19–23. Special Agent Thomas Maguire—who attended the briefing, participated in the search of the NYGG offices, and later took over for Agent Komar as the case agent on the Wey investigation—characterized the briefing as providing a "big-picture overview" of what was presented as a "fairly typical securities fraud case." *Id.* at 239:17–21.

At the Hearing, Agent Komar could not recall any instructions or guidance provided to the search team as to any sorts of items that should *not* be seized during the forthcoming search. *Id.* 190:13–16. The team was instructed, however, that the office of NYGG's in-house legal counsel was off-limits and could not be searched during the operation. *Id.* 239:22–240:2.

Also during the pre-search briefing, Agent Komar shared copies of the Operations Order with each member of the search team, and communicated to the team that the NYGG Warrant and the Komar Affidavit were "available" if anyone would like to review them personally. *Id.* 123:15–16, 125:2–126:6, 240:6–22. There is no credible evidence, however, that any agent other than Komar himself did in fact review the Komar Affidavit in advance of the search. Agent Komar testified that he "did not hand out copies" of the Komar Affidavit to the team, and "did not make sure every single person read" it. *Id.* 125:13–126:4. In addition, while Komar first testified at the Hearing to his vague belief that he at some point e-mailed the Komar Affidavit to members of the FBI team, subsequent searches by the Government identified no such e-mail communications. *Id.* 125:13–22, 228:14–230:4. AUSA Massey, for his part, expressed "doubt" that he read any portion of the Komar Affidavit directly to the search team. *Id.* 68:25–71:17. Agent Komar testified generally that at least one (unidentified) member of the search team did in fact review some portion of the Komar Affidavit; AUSA Massey, on the other hand, had no such recollections. *Id.* 68:25–71:17,

126:5–7, 185:12–20. The Government called no witnesses —other than Komar himself—who could definitively testify that they personally reviewed the Komar Affidavit prior to the search operation, and the Court cannot find that any such review took place.

Agent Komar conceded at the Hearing that the planned search of the NYGG offices could have been scheduled on any date up to 10 days after the briefing to afford all members of the search team an opportunity to review the Komar Affidavit, but that the FBI elected to go forward with the search the following morning. *Id.* 186:6–25.

2. Search of NYGG Offices

On the morning of January 25, 2012, the search team assembled for a final pre-operation briefing at the FBI's Manhattan offices to discuss logistics for the search. Hearing Tr. 126:10–16. AUSA Massey did not attend that meeting. *Id.* 126:17–18.

The search of the NYGG offices (the "NYGG Search") began shortly before 9:30 AM. *Id.* 126:19–127:1; Gov't Ex. 5. NYGG's suite consisted of an outer reception area surrounded on two sides by approximately nine individual offices, conference rooms, and a kitchen, together forming an "L" shape. Gov't Ex. 4 (NYGG Office Layout Diagram); Hearing Tr. 243:13–16. Wey and all other NYGG employees present in the office when the ***369** NYGG Search began were gathered into one of the conference rooms by FBI personnel and interviewed briefly to obtain basic contact information and background on their roles at NYGG. Hearing Tr. 127:4–9, 131:21–132:8, 243:18–23. Members of the FBI search team had copies of the NYGG Warrant, including its attachments, with them onsite, *id.* 127:23–25, 244:13–18, but there is no evidence that anyone other than Komar himself had a copy of the Komar Affidavit. Neither Wey nor any other employee on the scene was provided with a copy of the Komar Affidavit. *Id.* 46:8–17.

Agent Komar, serving as the team leader, personally searched the reception area in the outer portion of the office and then remained in that area, ostensibly to field any questions from other agents. Although Komar himself testified generally that team members asked him questions on several occasions, he recalled only one specific inquiry as to whether a particular document fell within the scope of the NYGG Warrant. *Id.* 128:1–19, 130:7–131:6, 132:9–10. The Government presented no other evidence at the Hearing suggesting that the searching agents addressed questions to Agent Komar. The Court is likewise aware of no evidence that Agent Komar in any way directly supervised, reviewed, or spot-checked the team's seizure decisions.

AUSA Massey was not onsite during the NYGG Search but communicated during the course of the Search with, at least, Agent Komar. *Id.* 16:4–8. At the Hearing, AUSA Massey could not recall having any discussions with Agent Komar or his team as to whether particular items fell within the scope of the NYGG Warrant, and agreed that it was generally up to the searching agents' "discretion" to make any such determinations. Hearing Tr. 67:18–68:20. From his own perspective, AUSA Massey testified, "all records of [NYGG] ... were in play," *id.* 14:8–10, largely because the Government "needed to understand the entire business, even if some part of the business was legitimate," in order to properly assess its role as a source of income to Wey, *see, e.g., id.* 36:1–12 (citing Government's suspicion that Wey was "making way too much money to be accounted for by [NYGG's advisory fees])." When pressed to cite any types of materials *not,* in his view, covered by the NYGG Warrant, AUSA Massey offered only medical prescriptions, illegal drugs and paraphernalia, child pornography, and terrorist manifestos. *Id.* at 47:17–48:10. (Although Massey also later testified that he would deem "a bag of heroin ... found on the premises" that "said New York Global Group" on it "within the scope of the warrant." *Id.* 50:13–16.)

Approximately twelve or thirteen of Komar's colleagues conducted the physical searches of NYGG's individual offices and other rooms. *See, e.g., id.* 127:10–22, 243:24–244:9; Gov't Ex. 1; Gov't Ex 5. Of these agents, only Agent McGuire testified at the Hearing. Agent McGuire recalled personally searching one of NYGG's "larger" individual offices and deciding whether to seize documents by comparing their contents to the list of individuals and entities set forth in Exhibit B to the NYGG Warrant (which, of course, included NYGG itself). He testified that, while it was possible that he sought a second opinion from another agent on the search team at some point, he did not recall "coming across documents where [he] had a difficult time determining whether it was covered by the search warrant." *Id.* 243:17–247:23. Asked whether he remembered deciding *not* to seize any particular materials, Agent McGuire testified that he recalled determining that a set of resumes belonging to people who were apparently applying for jobs at NYGG were "not pertinent to the ***370** investigation."

Id. 245:18–248:19. He also testified that he made that determination without consulting any of his colleagues, agreeing that it was a "clear decision" that such documents were "not responsive." *Id.* 298:13–299:1. Notwithstanding Agent McGuire's conclusion, resumes of NYGG applicants (whose names did not appear in the NYGG Warrant or Komar Affidavit) were in fact seized during the course of the NYGG Search. *See, e.g.,* Supplemental Memorandum of Law in Support of Defendant Benjamin Wey's Motion to Suppress, Dkt. No. 95 ("Def. Supp. Br.") Ex. B.

According to Agent Komar, the total volume of paper records found in the NYGG offices was—consistent with the Government's expectations going in—less than substantial. *Id.* 133:14–134:13. He testified that the team had sufficient time during the NYGG Search to review essentially every page of every document found, and estimated that, in total, the team ultimately seized approximately 4,500 pages of hard-copy documents. *Id.; see also* Gov't Ex. 6 (Evidence Recovery Log from NYGG Search noting seizure of approximately thirteen redwelds, boxes, envelopes, and discs). Komar personally recovered only one redweld of documents; the balance was seized by other members of the search team. Gov't Ex. 6. Asked at the Hearing to compare the hard-copy search fruits to the overall volume of paper records found or reviewed, Agent Komar could not provide specifics but testified: "We didn't take every single piece of paper, but there really wasn't much paper to start with either." Hearing Tr. 134:5–13.

Computer equipment and electronic devices found during the NYGG Search were assessed by CART personnel to determine whether onsite searches or data copying would be feasible. *Id.* 134:14–135:13. The team ultimately deemed these options impractical with respect to the vast majority of the items. *Id.; see also* Gov't Ex. 7 (CART On–Site Search Form for NYGG Search). With the exception of Wey's cell phone, which the search team seized, CART personnel copied or digitally imaged the cell phones of all NYGG employees present in the office during the NYGG Search. The balance of the electronic materials found, however, including all laptop computers, flash drives, and hard drives from desktop computers, were seized for offsite review. Hearing Tr. 134:14–135:13, 175:22–177:6; Gov't Ex. 7. In total, the team copied or seized approximately 24 pieces of computer or other electronic equipment. Gov't Ex. 7. With respect to NYGG employees' cell phones, at least, the search team did not make any onsite determination as to whether the devices related in any way to the individuals and entities set forth in Exhibit B to the NYGG Warrant; rather, the cell phones of all those present in the office were indiscriminately imaged (or seized) for later review. Hearing Tr. 176:2–6.

The NYGG Search lasted approximately four to five hours, concluding shortly before 3:00 PM. Hearing Tr. at 181:7–9; Gov't Ex. 5.

3. Search of Wey Apartment

At the time it applied for the NYGG Warrant, the Government had reason to believe, at least, that stock certificates potentially implicated in Wey's purported scheme had at some point been sent to the Wey Apartment. Hearing Tr. 181:24–l 82:11 (Agent Komar acknowledging that the Komar Affidavit asserted as much). It did not, however, seek a search warrant for that location until the NYGG Search was in progress. *Id.* As alluded to above, at some point during the "early stages" of the NYGG Search, Agent Garwood of the FBI learned from interviews of NYGG employees that Michaela Wey served as NYGG's bookkeeper and office manager and generally ***371** completed her work from the Wey Apartment. Hearing Tr. 16:15–25, 135:14–24, 182:8–11. Upon receiving that additional information and with the NYGG Search having turned up none of the stock certificates of interest, AUSA Massey, along with Agent Garwood, drafted the Garwood Affidavit and applied for the Apartment Warrant. Hearing Tr. 17:1–18, 135:25–136:5, 181:10–183:23.

With the application process in motion, Agent Komar instructed FBI personnel, including several agents already onsite at the Wey Apartment, to serve grand jury subpoenas on Michaela Wey, to secure the exterior of the Wey Apartment in order to ensure that no evidence would be removed or discarded. Hearing Tr. 136:6–13, 138:15–20, 253:9–254:7; Def. Ex. 16 (February 22, 2012 Memorandum of Agent Komar). The Court is aware of no evidence, however, that Komar or anyone else had any basis to believe that such activities were likely to take place.

After the Apartment Warrant issued, FBI personnel entered the Wey Apartment at approximately 4:30 PM and commenced a search (the "Apartment Search"). Hearing Tr. 138:8–24, 254:8–18; Gov't Ex. 12 (FBI Crime Scene Sign–In Log for Apartment Search); Def. Ex. 16. Ultimately, approximately seventeen FBI agents participated in the Apartment Search in some capacity. Gov't Ex. 12. Most, but not all, of these individuals had also participated in the

NYGG Search. *Compare* Gov't Ex. 5 *with* Gov't Ex. 12. No pre-operation briefing was conducted in advance of the Apartment Search. Hearing Tr. 300:18–20. There is also no evidence that any operations order or similar document was prepared to help guide the team in executing that Search.

Agent McGuire, who conducted an initial walkthrough at the outset of the Apartment Search, testified that he "briefly" reviewed the Apartment Warrant before beginning the Apartment Search. *Id.* 254:12–25, 257:2–9. He did not, however, review the Garwood Affidavit, and testified that he was not aware of any FBI personnel possessing a copy of the Garwood Affidavit during the course of the Apartment Search. *Id.* 301:3–10. Agent McGuire testified repeatedly that, to his understanding at least, the team was authorized to seize from the Wey Apartment, among other things, "any record we would find related to [Wey] finances," regardless "of date or time frame." Hearing Tr. 276:12–20, 304:11–14, 306:18–19.

Once again, Agent Komar, who arrived on the scene at approximately 4:50 PM, functioned as the team leader during the Apartment Search. Hearing Tr. 138:25–139:1; Gov't Ex. 12. And once again, Agent Komar testified generally at the Hearing that he was asked unspecified questions by unnamed agents about whether unidentified documents were "relevant to the search warrant." Hearing Tr. 139:2–139:10. As in the context of the NYGG Search, however, the Government called no members of the search team who could testify to having consulted Komar with respect to seizure decisions.

Within the Wey Apartment, the search team identified one "office area" with a "large amount of documents," but otherwise did not locate any rooms with a "substantial" number of hard-copy documents. Hearing Tr. 139:5–140:3. Agent Komar personally assisted in searching "what appeared to be a guest room" and the rooms of Wey's children and then "focused [the team's] attention on the office area." *Id.* 139:14–25. AUSA Massey, once again, was not onsite for the Apartment Search, but did communicate with unidentified agents conducting the search by phone and e-mail. Hearing Tr. 19:13–16.

***372** During the course of the Apartment Search, the search team did not review every document that it encountered. Instead, the searching agents would "flip through" any given box or other container to see if it contained at least a "subset" or "sampl[e]" of relevant documents, and, if so, they would seize the entire container. *See* 146:5–147:9, 155:2–156:21 (Agent Komar also describing the process as allowing the team to "get a little bit of comfort" that it was not seizing documents "outside of the scope" of the Apartment Warrant). At the Hearing, Agent Komar attributed that strategy to "the sense of urgency" purportedly created by the FBI's desire not to "disrupt someone's life," especially with the Weys' children apparently expected back at the Wey Apartment sometime in the late afternoon or early evening. *Id.* Agent McGuire likewise testified that Michaela Wey "was upset about th[e] search and ... very concerned about her kids coming soon," and that, "towards the end of the search there was some tension because she wanted the search to wrap up" and the agents "out of her apartment." *Id.* 255:5–9, 257:13–20. To address the concerns about the children, Agent McGuire and his colleagues ordered the Apartment Search to target the children's bedrooms and play area first, so that the children could be "segregated" from the search of the remainder of the Wey Apartment's rooms once they returned home with their nanny. *Id.* 255:19–256:4.

Ultimately, the search team seized approximately 4,000 hard-copy documents from the Wey Apartment. Komar Dec. ¶ 13. That represented something less than the total number of documents found during the Apartment Search. Hearing Tr. 147:6–9; *see also* Gov't Exs. 15, 15A–15H (FBI entry and exit photographs of Wey Apartment). As cataloged by the FBI, the total hard-copy take from the Wey Apartment consisted of approximately twenty-eight discrete sets of materials, including boxes, redwelds, discs, videos, a suitcase, and other things. Gov't Ex. 13 (Evidence Recovery Log from Apartment Search). As presented to the Court at the Hearing, the hard-copy materials taken from the Wey Apartment partially filled 17 boxes, as well as additional manila envelopes, redwelds, and a suitcase. Hearing Tr. 257:25–261:12. Agent Komar personally recovered only one of these sets of documents. Gov't Ex. 13. Agent McGuire did not participate in the search for "individual items" and did not personally recover anything. *Id.*; Hearing Tr. 257:2–9.

Several documents were seized, at least occasionally in tom or otherwise physically compromised form, from wastebaskets and from a trash bag that was located within the noted suitcase, which itself was found in a hallway closet. Hearing Tr. 142:10–145:4, 155:19–156:21, 160:9–18. The team encountered certain documents in these locations that were intermingled with trash, difficult to decipher, or otherwise "burdensome" to analyze onsite, and responded by removing entire sets of documents for offsite review, pursuant to a decision reached by Agent Komar, his supervisor, and

AUSA Massey. *Id.* 142:10–145:4, 155:19–156:21, 160:9–18, 167:21–168:11. Although the FBI later sorted out from these sets certain materials that it deemed beyond the scope of the Apartment Warrant, it maintained custody of those materials and to date has not returned them to the Weys. *Id.* 169:23–170:6.

Documents taken from the Wey Apartment included many of a personal nature, such as pharmaceutical prescriptions and related documents; materials reflecting information on medical appointments and examinations; X-rays of Wey family members; Wey's living will and health care directives; recreational sports schedules; documents, photographs and other mementos ***373** from Michaela Wey's secondary school, collegiate and law school careers; children's scholastic records and test scores; divorce papers from Wey's first marriage dating to the late 1990s; passports belonging to the Weys' children and other apparent family members; family photographs; and photographs of rural landscapes, among other things. *See, e.g.,* Hearing Tr. at 167:4–169:19, 265:24–276:11; Def. Supp. Br. Exs. A, C. During the Hearing, Government witnesses offered post-hoc justifications for some of these seizures that the Court found unpersuasive. For example, AUSA Massey testified that a medical prescription information sheet for the Weys' child would have been within the scope of the Apartment Warrant if it reflected "pricing information" or "cost information" because they could go to the Weys' "personal expenses." Hearing Tr. 55:13–57:7. He also asserted that PSAT scores of the Weys' child would have been seizable if the score report "indicated where he would attend school." *Id.* 58:24–59:5. Additionally, newspaper clippings on Michaela Wey's collegiate tennis career were within the scope of the Apartment Warrant as long as they were found in a file with other documents that showed how the Weys first met in Oklahoma. *Id.* 59:25–60:7. Agent Komar found a document confirming a dentist appointment for Michaela Wey responsive to the Warrants because "Michaela Wey's address is of relevance." *Id.* 167:10–18. Agent McGuire, for his part, characterized divorce records from Wey's prior marriage seizable "if they talk about financial arrangements" because "then they would relate to financial records." *Id.* 304:24–305:5.

With regard to certain other personal documents, Agent McGuire (who was not the individual who made the seizure determinations during the Apartment Search) noted that they were found mixed in boxes or redwelds with financial and other documents that he would have deemed responsive to the Apartment Warrant and explained that seizure of the entire container would be justified to ensure the "integrity" of the documents. Hearing Tr. 265:24–276:11. Still other personal documents—most notably, medical X-rays and related records—were simply conceded by Government witnesses to fall outside the scope of the Apartment Warrant. *See, e.g., id.* 59:6–9, 277:9–19.

Most, if not all, of the electronic devices and computer equipment found within the Wey Apartment, including Michaela Wey's personal cell phone, were seized; any others were copied or imaged onsite. *See, e.g.,* Komar Dec. ¶ 14; Hearing Tr. 178:5–179:15; Def. Ex. 16. By the Court's count, at least 25 devices or pieces of equipment were seized or copied in total, including cell phones, personal computers, laptops, and flash drives. Def. Ex. 14 (in pertinent part, FBI Receipts for Property Received/Returned/Released/Seized from Wey Apartment); Komar Dec. ¶ 14. The FBI's effort to image or copy electronic evidence onsite was at least somewhat more limited than it had been during the NYGG Search earlier that day, in part due to the fact that only one CART agent participated in the Apartment Search—several fewer than had participated in the NYGG Search. Hearing Tr. 178:5–179:15.

The Apartment Search concluded at approximately 9:00 PM. Hearing Tr. 257:10–12; Gov't Ex. 12.

4. Post–Search Developments

a. Retention or Return of Seized Materials

In approximately February 2012, the FBI, at least partially in response to requests from NYGG's and Wey's counsel, copied all electronic devices and computer equipment seized during the NYGG Search and the Apartment Search (together, ***374** the "Searches") and returned either the original devices or images of their data to NYGG and Wey. Komar Dec. ¶ 15; Hearing Tr. 20:23–21:18, 147:13–148:14. In May 2012, counsel further requested in writing the return of all hard-copy materials taken from both locations. *See* Siegal Dec. Ex. 37, Dkt. No. 46–39. Copies of at least some of the hard-copy materials were provided to counsel for Wey and NYGG by the prosecution team sometime in the fall or winter of that year. Komar Dec. ¶ 16; Hearing Tr. 169:23–170:6, 219:10–221:14; Def. Ex. 5 (internal Government e-mail correspondence discussing status of copying effort). The FBI retained custody of—and, to the Court's understanding, does to this day—substantially all original hard-copy materials

and all electronic data, regardless of whether it had deemed them responsive to the relevant Warrant. *See, e.g.,* Hearing Tr. 99:12–100:11, 169:23–170:6, 180:11–24, 334:20–335:21.

b. Processing, Review, and Handling of Electronic Materials

After copying the seized electronic devices for return to NYGG and Wey, the FBI CART team processed the digital data and loaded it onto its review platform. *See, e.g.,* Hearing Tr. 21:19–22:6, 148:15–20. Due to the sheer volume of the electronic search take—which Agent Komar estimated to include about eighteen terabytes of data—Agent Komar worked with the CART team to process and load the documents on a rolling basis according to tranches of priority. *Id.* 148:21–149:9.

Based on its understanding that NYGG and/or the Weys could have potential privilege claims with respect to some of this material, AUSA Massey and Agent Komar organized a so-called "taint review" by an FBI wall team to segregate non-privileged from potentially privileged documents in advance of the case team's substantive review of the material. *See, e.g., id.* 22:12–25:13, 82:3–83:10, 149:10–25, 193:25–195:4, 280:1–10. To that end, Massey and Komar compiled—with substantial written input from NYGG's and/or Wey's counsel—a lengthy list of the names and e-mail addresses of attorneys who had at some point represented NYGG or the Weys. *Id.*; Gov't Exs. 17–18 (e-mail correspondence concerning attorney list); Komar Dec. ¶ 18. Correspondence between NYGG's counsel and Massey pertaining to the list lasted until at least early June 2012, and the list itself, which grew to include dozens if not hundreds of attorneys, was still subject to revision as of at least early August 2012. Gov't Exs. 17–18; Hearing Tr. 23:4–24:1, 280:20–281:5. The taint review itself was conducted by three FBI agents working on an intermittent basis between June 2012 and approximately December 2012. Komar Dec. ¶¶ 19–20; Hearing Tr. 24:25–25:13, 150:7–152:11, 195:5–7. AUSA Massey testified that, during this period of time, he was concerned about the pace at which the review was proceeding, especially in light of emergent district court case law requiring the Government to review and make use of digital search takes within a reasonable period of time. *Id.* 24:2–13, 84:13–18, 86:1–8 (citing Judge Irizarry's then-recent decision in *United States v. Metter,* 860 F.Supp.2d 205 (E.D.N.Y. 2012)). Nevertheless, it is evident from the record that the taint review proceeded slowly. Massey e-mailed his supervisor on August 28, 2012, for example, to note, among other things, "We seized the NYGG hard drives etc. seven months ago and this privilege review is nowhere near finished." Def. Ex. 5.

As the taint review was completed on a rolling basis, the Government began, in late 2012 or early 2013, to conduct a substantive review of the non-privileged materials. Hearing Tr. 25:14–23, 152:2–11; Komar Dec. ¶ 21; *see also* Def. Ex. 6 ***375** (January 15, 2013 e-mail from AUSUA Massey to colleagues noting that "[t]he FBI has now started reviewing the electronic records after a long delay."). In the first instance, Agent Komar personally attempted to search the materials using keywords, some of which may "very well" have not appeared on Exhibit B to the Warrants (the list of individual and entities to which, theoretically, materials would have to relate in order to be seizable). Komar Dec. ¶ 21; Hearing Tr. 152:13–16, 201:10–14. He quickly encountered "difficulty" in using the search program available, however. Komar Dec. ¶ 21; Hearing Tr. 152:13–16. In response, he shifted gears and began a "file-by-file review" of some of the seized flash drives, making determinations as to the "pertinence" of individual documents. Komar Dec. ¶ 21; Hearing Tr. 152:16–21, 153:10–20. Agent Komar was not assisted in his review by any other agents, and was never given any sort of deadline for completion. Hearing Tr. 199:12–200:5. Ultimately, he was unable to make notable headway before he was transferred in February 2013 to a position at FBI headquarters in Washington, D.C. Komar Dec. ¶¶ 21–22; Hearing Tr. 153:7–8, 153:21–154:3, 198:18–199:11.

Following Komar's transfer, Agent McGuire took over as case agent. Komar Dec. ¶ 22; Hearing Tr. 154:4–5. To familiarize himself with the broader investigation, Agent McGuire reviewed the case file and Komar and Garwood Affidavits, among other things. Hearing Tr. 279:10–19. By sometime in March 2013, McGuire was prepared to begin his own substantive review of the non-privileged electronic materials taken during the Searches. Hearing Tr. 281:11–14.

To facilitate Agent McGuire's review of the electronic materials, AUSA Massey developed a list of search terms. Hearing Tr. 26:1–27:10, 282:3–18; Gov't Ex. 19 (search term list as of May 3, 2013). Massey developed the list by "start[ing]" with Exhibit B to the Warrants and then "add[ing] names that [Massey] believed were tied directly or tied to the names in the search warrant." Hearing Tr. 26:18–20; *see also* Def. Ex. 10 (May 3, 2013 e-mail from Massey to McGuire and others noting that the "majority of the [search] terms are

in the search warrant application," and the "others are directly related to items listed in the search warrant"). As Massey conceded at the Hearing, however, he assessed "relatedness" with the "benefit of 15 month[s'] more investigation time" following the Searches themselves. Hearing Tr. 113:10–15. Indeed, Massey testified, for example, that to the extent he "learned ... information" about individuals identified in the Warrants "in the intervening period" between the Searches and the development of the search term list, it would have been "acceptable to add that [information] to the list." *Id.* 114:2–10. There is no dispute that Massey's list, which was provided to Agent McGuire in early May 2013, included dozens (if not more) of names that were not included in Exhibit B to the Warrants or that Agent McGuire was well aware of that when he received the list. *See, e.g.,* Def. Ex. 10, Hearing Tr. 91:5–92:1, 98:6–10, 283:3–18, 310:14–311:2, 315:22–316:11. For example, the name of Wey's co-Defendant in this matter, Seref Dogan Erbek, appeared on Massey's search term list but did not appear on Exhibit B. *See* Gov't Ex. 19; Hearing Tr. 93:7–94:15. The search term list developed by Massey was not submitted to a Magistrate Judge for approval as an expansion of the original Searches. Hearing Tr. 92:2–16.

At approximately the same time that he provided the search term list to Agent McGuire to aid in his review of the electronic Search fruits, AUSA Massey also shared, at McGuire's request, an e-mail ***376** memorandum summarizing the Government's possible charging theories with respect to Wey as of May 2013 (almost 16 months after the Warrants were executed). Def. Exs. 10, 22 (May 2013 e-mails between Massey and McGuire, among others); Hearing Tr. 312:11–314:8. McGuire asked for the summary to help guide his review of the electronic documents and to assist him in identifying "the most critical evidence" or "hot docs." Hearing Tr. 313:13–314:8, 361:24–362:12. Massey's memorandum highlighted, in addition to the " '[b]eneficial [o]wnership' fraud" theory described in sum and substance in the Komar Affidavit and the Operations Order, an "alternate" theory of "tax evasion" in connection with fund transfers between Wey's sister and Wey's wife. Def. Ex. 22. Notably, neither the Komar Affidavit, nor the Warrants, nor the Operations Order referenced any active investigation of Wey pertaining to tax evasion or tax fraud.[3] Indeed, Agent McGuire testified that he personally suggested the new tax fraud theory to the prosecution team after taking over as case agent in 2013 (more than a year after the Searches), and that he had discussions about the theory with Internal Revenue Service personnel during that timeframe. Hearing Tr. 353:7–358:3. Massey's memorandum also noted that "much of the evidence" marshalled therein came from proffer sessions that—according to Agent McGuire's Hearing testimony—"probably" took place sometime after the Warrants were executed. Hearing Tr. 326:6–327:4; Def. Ex. 22.

In early May 2013, after receiving the search terms and theories-of-the-case memorandum from AUSA Massey and rereading at least one of the Warrants, Agent McGuire began his review of the electronic materials. Hearing Tr. 284:9–15, 315:19–21. Notwithstanding Agent Komar's limited foray into a portion of the electronic documents, Agent McGuire "started from scratch," and did a "complete review" of the confiscated materials. *Id.* 307:16–308:16. His review took place predominantly at FBI offices in New Jersey across the span of ten full-day sessions. 284:16–285:5, 286:11–14, 289:25–290:7. McGuire testified at the Hearing that, to his understanding, his task was to use the search terms provided by AUSA Massey to locate and "tag" as "pertinent" any documents within the electronic Search fruits that were "covered by the search warrant." Hearing Tr. 283:19–284:8, 308:17–309:4. Such documents could include, for example, any "financial records related to [NYGG]" or any "e-mails with NYGG." *Id.* 293:6–18. There is no evidence that Agent McGuire referenced or otherwise considered the Komar or Garwood Affidavit while conducting his review.

Agent McGuire worked systematically through the May 2013 list of search terms ***377** provided by AUSA Massey, running each term across two separate FBI databases containing materials recovered from NYGG and the Wey Apartment, respectively. *See, e.g.,* Gov't Ex. 16 (list of search terms with Agent McGuire's contemporaneous handwritten notes); Hearing Tr. 327:5–329:19. On occasion, Massey supplemented the list with additional search terms, and McGuire also developed novel terms based on his review of the documents. Hearing Tr. 330:10–17, 331:11–20. Sometimes McGuire determined that certain search terms yielded "too many false positives" in its returns and were thus ineffective and should be discarded. *Id.* 286:15–288:10, 293:23–294:3; *see also* Gov't Ex. 16. Conversely, if Agent McGuire made a preliminary determination based on "10 or 15" documents that a particular search term appeared to reliably return documents that actually pertained to the search term's intended referent, he would then proceed to tag all documents returned by the relevant search as pertinent, without necessarily engaging in further substantive review on a document-by-document basis. Hearing Tr. 289:1–20; 292:9–294:3. At least one of the novel search terms that

McGuire ran was intended to identify tax-related documents and was developed in cooperation with IRS personnel. *Id.* 353:7–358:3.

Agent McGuire testified that running the search terms across the two databases was a lengthy process, with each individual search through one of the databases taking as long as two to three minutes. *Id.* 290:1–22. Like Agent Komar before him, Agent McGuire performed his review without substantive assistance or support from any other agents. *Id.* 291:2–5.

McGuire completed his review in approximately early September 2013. *Id.* 291:6–8, 330:21–331:1, 333:22–334:2. In total, he tagged approximately 14,000 electronic documents from the Apartment Search and slightly over 90,000 electronic documents from the NYGG Search as pertinent. *Id.* 291:22–292:2, *see also id.* 334:14–16 (estimating overall total of about 105,000). He provided copies of all such documents to the prosecution team. 291:9–21, 329:21–25.

Wey was not indicted for another two years. During that time and to this day, the FBI retained all electronic materials taken from NYGG and the Wey Apartment (whether in original or copied form), regardless of whether they had been identified as pertinent during McGuire's review. The Government did not introduce any evidence at the Hearing that would help explain the reasons for such broad retention.

In the weeks leading up to Wey's indictment (roughly late August to early September 2015), FBI personnel conducted additional searches across all electronic materials recovered from both locations. Those searches were the subject of substantially inconsistent Hearing testimony by the FBI agents involved. Agent McGuire, who remained the case agent during the relevant timeframe, testified in sum and substance that in August or September 2015, the FBI was seeking in anticipation of Wey's indictment to prepare clean "evidence copies" of specific pertinent documents that had been identified during the 2013 review, but learned that the materials taken during the Searches had apparently lost their electronic privilege and pertinence tags due to a technical malfunction. Hearing Tr. 337:6–341:7, 349:6–353:1, 358:8–361:4. Agent McGuire concluded that it would be inappropriate for agents involved in the investigation to personally conduct searches through the unsegregated FBI databases as of 2015, and decided instead to recruit an uninvolved taint agent, Elizabeth Miller, to ***378** perform the necessary searches instead. *Id.* According to McGuire, Agent Miller was specifically tasked with finding electronic copies of only certain of the "exact same document[s]" that the FBI had already deemed pertinent and non-privileged in 2013 and, to that end, he provided her with hard copies of all the relevant documents and instructed her to run search terms consisting of direct "quote[s]" and other "snippets" from those documents, many of which pertained to Defendant Erbek. *Id.* McGuire testified that Agent Miller did not identify any additional documents of interest through this effort beyond what the FBI had tagged as pertinent in 2013. *Id.*

In response to Agent McGuire's testimony at the Hearing, the defense called Agent Miller, who had not expected to testify and initially was not present in the courthouse. Agent Miller agreed that she was brought in nominally as a taint agent in 2015—having had no prior involvement in the investigation of Wey—in order to run searches through the FBI's preexisting databases. She testified, however, that Agent McGuire provided her with five to ten search terms, each approximately one to two words in length, along with "only a few ... examples" of documents "that could potentially have information that they would want" and directed her to search for "similar" documents within the databases. Hearing Tr. 368:13–375:23, 377:3–9. She specifically recalled that Defendant Erbek's name was among the search terms provided by Agent McGuire. *Id.* When asked about using Erbek's name as a search term, Agent McGuire testified that, in his view, all documents referencing Erbek were responsive to the Warrants—notwithstanding that, as noted, neither the Affidavits nor the Warrants made any reference to him—because McGuire "learned through the investigation in review of the documents" that Erbek had facilitated financial transactions for Wey and his sister and, as such, materials bearing his name would constitute "financial records relating to Benjamin Wey." *Id.* 350:14–351:23.

Agent Miller testified that, prior to commencing the requested searches, she "was given just a very brief summary of the case" and thus "had some knowledge of what [she] ... should be looking for," but "was not given a full scope of what the search warrant entailed." *Id.* 376:1–8. Ultimately, according to Agent Miller, she identified and electronically tagged "possibly" as many as fifty or more documents in the databases that she viewed as similar to the examples provided. *Id.* 374:13–375:23. A contemporaneous e-mail authored by Agent McGuire suggests that Agent Miller "located" as many as "150 documents" of relevance, subject to further privilege review. Def. Ex. 20 (August 20, 2015 e-mail from McGuire to AUSAs and others). Agent Miller did not, however, play any

role in transmitting any of those documents to McGuire or the prosecution team and was unsure if any such transmission ever occurred. *Id.* 378:14–379:18.

The Court is unable to reconcile Agent McGuire's version of these events with that of Agent Miller. Having observed both witnesses at the Hearing and after careful consideration of their respective testimony, the Court credits the testimony of Miller, an agent with no particular professional stake in this matter who offered clear and internally consistent recollections despite being called to the stand unexpectedly and testifying with negligible preparation and unaware of the questions bearing on Wey's motion. McGuire, by contrast, served as case agent on the FBI's Wey investigation and was featured at the Hearing as one of the Government's primary witnesses, evincing thorough preparation—including on this particular point—and ***379** a keen sensitivity to the legal issues in play throughout the proceedings.

As noted, Wey was indicted in early September 2015. The instant motion was filed along with a slew of other pretrial motions—which the Court has resolved by separate Order—in mid–2016.

II. Discussion

Wey contends primarily that the fruits of the Searches must be suppressed because the Warrants are insufficiently particularized, overbroad "general warrants," and because the Government's lengthy (and continuing) retention and indiscriminate review of the vast trove of confiscated electronic materials must be deemed unreasonable under the circumstances.[4]

A. Constitutional Requirements for Search Warrants

The Fourth Amendment to the United States Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV.

"The Fourth Amendment's requirements regarding search warrants are not 'formalities.' " *United States v. Voustianiouk,* 685 F.3d 206, 210 (2d Cir. 2012) (quoting *McDonald v. United States,* 335 U.S. 451, 455, 69 S.Ct. 191, 93 L.Ed. 153 (1948)). "The chief evil that prompted the framing and adoption of the Fourth Amendment was the 'indiscriminate searches and seizures' conducted by the British 'under the authority of general warrants.' " *United States v. Galpin,* 720 F.3d 436, 445 (2d Cir. 2013) (quoting *Payton v. New York,* 445 U.S. 573, 583, 100 S.Ct. 1371, 63 L.Ed.2d 639 (1980)). "To prevent such 'general, exploratory rummaging in a person's belongings' and the attendant privacy violations, the Fourth Amendment provides that a 'warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity.' " *Id.* (internal citations omitted) (quoting *Coolidge v. New Hampshire,* 403 U.S. 443, 467, 91 S.Ct. 2022, 29 L.Ed.2d 564 (1971); *Kentucky v. King,* 563 U.S. 452, 459, 131 S.Ct. 1849, 179 L.Ed.2d 865 (2011)). The particularity requirement "is necessarily tied to the ... probable cause requirement." *In re 650 Fifth Ave. & Related Props.,* 830 F.3d 66, 98 (2d Cir. 2016). That is because " '[b]y limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character ***380** of the wide-ranging exploratory searches the Framers intended to prohibit.' " *Id.* (quoting *Maryland v. Garrison,* 480 U.S. 79, 84, 107 S.Ct. 1013, 94 L.Ed.2d 72 (1987)). In assessing the Constitutional sufficiency of any warrant, courts must be mindful that "the ultimate touchstone of the Fourth Amendment is 'reasonableness.' " *Brigham City, Utah v. Stuart,* 547 U.S. 398, 403, 126 S.Ct. 1943, 164 L.Ed.2d 650 (2006) (internal citation omitted).

1. Particularity

"Courts implement the particularity requirement by insisting that warrants not 'leave to the unguided discretion of the officers executing the warrant the decision as to what items may be seized.' " *United States v. Zemlyansky,* 945 F.Supp.2d 438, 453 (S.D.N.Y. 2013) (quoting *United States v. Riley,* 906 F.2d 841, 844 (2d Cir. 1990) (citations omitted)). Put differently, "[a] warrant must be 'sufficiently specific to permit the rational exercise of judgment [by the executing officers] in selecting what items to seize.' " *United States v. Shi Yan Liu,* 239 F.3d 138, 140 (2d Cir. 2000) (brackets in original) (quoting *United States v. LaChance,* 788 F.2d 856, 874 (2d Cir. 1986) (internal quotation marks omitted)).

The Second Circuit has recognized that, to comport with the Fourth Amendment's particularity requirement, a warrant must satisfy three criteria. *See Galpin,* 720 F.3d at 445; *see also United States v. Ulbricht*, 858 F.3d 71, 98–99 (2d Cir. 2017). First, it must "identify the specific offense for which the police have established probable cause." *Galpin,* 720 F.3d at 445; *see also 650 Fifth Ave.*, 830 F.3d at 99 ("[F]or a warrant to meet the particularity requirement, it must identify the alleged crime for which evidence is sought."); *United States v. George*, 975 F.2d 72, 75–76 (2d Cir. 1992) (warrant permitting seizure of evidence "relating to the commission of a crime" was constitutionality infirm because "[n]othing on the face of the warrant tells the searching officer for what crimes the search is being undertaken"). Second, the warrant is required to "describe the place to be searched." *Galpin*, 720 F.3d at 445–46. And third, it must "specify the items to be seized by their relation to designated crimes." *Id.* at 446 (internal quotation marks omitted) (citing, *inter alia*, *United States v. Buck,* 813 F.2d 588, 590–92 (2d Cir. 1987) (warrant authorizing seizure of "any papers, things or property of any kind relating to [the] previously described crime" was insufficiently particularized insofar as it "only described the crimes—and gave no limitation whatsoever on the kind of evidence sought")); *United States v. Rosa,* 626 F.3d 56, 62 (2d Cir. 2010) (warrant "defective in failing to link the items to be searched and seized to the suspected criminal activity" because it "thereby lacked meaningful parameters on an otherwise limitless search"); *see also Ulbricht,* 858 F.3d at 98–99 (reciting same three requirements).[5]

***381** In addition to the foregoing, courts in this Circuit have identified certain "circumstance-specific considerations" that may bear on whether a given warrant lacks particularity, even if they do not constitute formal, universal requirements. *Zemlyansky,* 945 F.Supp.2d at 454. Many courts, for example, " 'have found warrants for the seizure of [business] records constitutionally deficient where they imposed too wide a time frame or failed to include one altogether.' " *Id.* (quoting *United States v. Cohan,* 628 F.Supp.2d 355, 365–66 (E.D.N.Y. 2009) (citing "general agreement that a time frame is *relevant*" even if not necessarily "required")); *see also United States v. Levy,* 11–cr–62, 2013 WL 664712, at *11 n.7 (S.D.N.Y. Feb. 25, 2013) ("Several courts in this Circuit have recognized the constitutional questions that are raised by the lack of a specific date range in a warrant for documentary records and warned the Government to include one when possible."); *cf. United States v. Hernandez*, 09–cr–625, 2010 WL 26544, *9 (S.D.N.Y. Jan. 6, 2010) ("A failure to indicate a time frame could render a warrant constitutionally overbroad because it could allow the seizure of records dating back arbitrarily far and untethered to the scope of the affidavit which ostensibly provided probable cause.") (internal quotation marks and alterations omitted).

Of some significance here, the Supreme Court established in its 2004 decision in *Groh v. Ramirez* that the Fourth Amendment "requires particularity in the warrant, not in the supporting documents," and, accordingly, "the fact that the warrant *application* adequately described the 'things to be seized' does not save the *warrant*" from failure to satisfy that requirement. 540 U.S. 551, 557, 124 S.Ct. 1284, 157 L.Ed.2d 1068 (2004) (emphasis in original). That is because the " 'presence of a search warrant serves a high function,' and that high function is not necessarily vindicated when some other document, somewhere, says something about the objects of the search, but the contents of that document are neither known to the person whose home is being searched nor available for her inspection." *Id.* (internal citation omitted) (quoting *McDonald,* 335 U.S. at 455, 69 S.Ct. 191). Included in that "high function" is not only the "prevention of general searches," but also the " 'assur[ance] [to] the individual whose property is searched or seized of the lawful authority of the executing office, his need to search, and the limits of his power to search.' " *Id.* (quoting *United States v. Chadwick,* 433 U.S. 1, 9, 97 S.Ct. 2476, 53 L.Ed.2d 538 (1977), *abrogated on other grounds, California v. Acevedo,* 500 U.S. 565, 111 S.Ct. 1982, 114 L.Ed.2d 619 (1991)).

Accordingly, "a court may construe a warrant with reference to a supporting ***382** application or affidavit" only "if the warrant uses appropriate words of incorporation, and if the supporting document accompanies the warrant." *Id.* at 557–58, 124 S.Ct. 1284. And, as the Second Circuit has concluded, "for an attached affidavit properly to be incorporated into a warrant, the warrant must contain 'deliberate and unequivocal language of incorporation' "—"[l]anguage in a warrant that simply references an underlying affidavit" does not suffice. *650 Fifth Ave.,* 830 F.3d at 99–100 (quoting *United States v. Walker,* 534 F.3d 168, 172–73 & n.2 (2d Cir. 2008) (*per curiam*)); *see also Rosa,* 626 F.3d at 64 (recognizing that after *Groh,* courts "may no longer rely on unincorporated, unattached supporting documents to cure an otherwise defective search warrant").

2. Probable Cause and Overbreadth

"The Supreme Court has explained that 'probable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules.' " *United States v. Falso,* 544 F.3d 110, 117 (2d Cir. 2008) (quoting *Illinois v. Gates,* 462 U.S. 213, 232, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983)). "In evaluating probable cause in any given case, a judge must make a practical common-sense decision whether, given all the circumstances set forth in the affidavit before him, there is a fair probability that contraband or evidence of a crime will be found in a particular place.' " *United States v. Raymonda,* 780 F.3d 105, 113 (2d Cir. 2015) (internal quotation marks and ellipsis omitted) (quoting *Gates,* 462 U.S. at 238, 103 S.Ct. 2317; *Falso,* 544 F.3d at 117). "Due to this subjective standard, a reviewing court generally accords 'substantial deference to the finding of an issuing judicial office that probable cause exists,' limiting [the] inquiry to whether the office 'had a substantial basis' for his determination." *Id.* at 113 (quoting *United States v. Wagner,* 989 F.2d 69, 72 (2d Cir. 1993)). "Nevertheless, under this standard, [courts] 'may properly conclude that ... a warrant was invalid because the [magistrate judge's] probable-cause determination reflected an improper analysis of the totality of circumstances.' " *Falso,* 544 F.3d at 117 (internal brackets omitted) (quoting *United States v. Leon*, 468 U.S. 897, 915, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984)).

The doctrine of overbreadth represents, in a sense, an intersection point for probable cause and particularity principles: it recognizes, in pertinent part, that a warrant's unparticularized description of the items subject to seizure may cause it to exceed the scope of otherwise duly established probable cause. Thus, "a warrant is overbroad if its 'description of the objects to be seized ... is broader than can be justified by the probable cause upon which the warrant is based.' " *United States v. Lustyik,* 57 F.Supp.3d 213, 228 (S.D.N.Y. 2014) (quoting *Galpin,* 720 F.3d at 446); *see also Ulbricht,* 858 F.3d at 102 ("breadth and particularity are related but distinct concepts" and a "warrant may be broad, in that it authorizes the government to search an identified location or object for a wide range of potentially relevant material," without necessarily "violating the particularity requirement"); *Zemlyansky,* 945 F.Supp.2d at 464 ("In determining whether a warrant is overbroad, courts must focus on 'whether there exists probable cause to support the breadth of the search that was authorized.' ") (quoting *Hernandez,* 2010 WL 26544, *8).

3. Additional Considerations in the Context of Electronically Stored Information

The fact that the Warrants at issue in this motion targeted—and the ***383** Search fruits ultimately consisted overwhelmingly of—electronically stored information implicates at least two additional considerations. First, as the Second Circuit has recognized, "[w]here ... the property to be searched is a computer hard drive, the particularity requirement assumes even greater importance." *Galpin,* 720 F.3d at 446. That is because the "seizure of a computer hard drive, and its subsequent retention by the government, can give the government possession of a vast trove of personal information about the person to whom the drive belongs, much of which may be entirely irrelevant to the criminal investigation that led to the seizure." *United States v. Ganias,* 824 F.3d 199, 217 (2d Cir. 2016) (*en banc*). As such, "[t]he potential for privacy violations occasioned by an unbridled, exploratory search of a hard drive is enormous"—a "threat [that] is compounded by the nature of digital storage." *Galpin,* 720 F.3d at 447. Indeed, the Government, once it has obtained authorization to search a hard drive, may in theory "claim that the contents of every file it chose to open were in plain view and, therefore, admissible even if they implicate the defendant in a crime not contemplated by the warrant," thus presenting a " 'serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant.' " *Id.* (quoting *United States v. Comprehensive Drug Testing, Inc.,* 621 F.3d 1162, 1176 (9th Cir. 2010)) (*en banc*) (*per curiam*); *cf. Riley v. California,* —— U.S. ——, 134 S.Ct. 2473, 2489–91, 189 L.Ed.2d 430 (2014) (recognizing that cell phones "differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person" owing to their "immense storage capacity" and their ability to "contain[ ] in digital form" both "many sensitive records previously found in the home" and "a broad array of private information never found in a home in any form—unless the phone is"); *Ganias,* 824 F.3d at 231 (Chin, J., dissenting) (noting that "[v]irtually the entirety of a person's life may be captured as data" on a computer or smartphone). Accordingly, a "heightened sensitivity to the particularity requirement in the context of digital searches" is necessary. *Galpin,* 720 F.3d at 447.

There is also the matter of the execution of a warrant targeting electronically stored information. Under Federal Rule of Criminal Procedure 41(e)(2)(B), a warrant may—

as the Warrants at issue did here—"authorize the seizure of electronic storage media or the seizure or copying of electronically stored information." Fed. R. Crim. P. 41(e)(2)(B). The Rule provides that "[u]nless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant." *Id.* Although "there is no established upper limit as to when the government must review seized electronic data to determine whether the evidence falls within the scope of a warrant," courts have recognized that "the Fourth Amendment requires the government to complete its review, *i.e.,* execute the warrant, within a 'reasonable' period of time." *Metter,* 860 F.Supp.2d at 215 (collecting cases); *see also United States v. Alston,* 15–cr–435, 2016 WL 2609521, at *3 (S.D.N.Y. Apr. 29, 2016) ("While Rule 41 prescribes no particular time period for data extraction in these circumstances, the time needed to complete off-site copying or review is subject to the rule of reasonableness."); *Lustyik,* 57 F.Supp.3d at 230 ("[l]ike all activities governed by the Fourth Amendment, the execution of a search warrant must be reasonable" and "[l]aw enforcement officers therefore must execute a search warrant," including when applicable review of recovered electronic communications, "within a reasonable ***384** time"); *cf. In the Matter of a Warrant for All Content and Other Information Associated with the Email Account xxxxxxx@ gmail.com Maintained at Premises Controlled by Google, Inc.,* 33 F.Supp.3d 386, 392 (S.D.N.Y. Aug. 7, 2014) (noting that courts have developed a "flexible approach" for assessing the execution of warrants for electronic evidence, applying a general standard of "reasonableness") (internal quotation marks omitted).

B. The Search Warrants Do Not Comport with the Requirements of the Fourth Amendment

1. The Search Warrants Lack Particularity

The Court has little difficulty concluding that, for several reasons, both the NYGG Warrant and the Apartment Warrant fail to describe the items to be seized with the requisite particularity. Because the Warrants are, as discussed above, substantially identical in their description of the items subject to seizure, the Court does not distinguish between them for purposes of this analysis.

a. Failure to Identify Suspected Crimes

First, on their face, both Warrants fail to set forth the crimes under investigation. As noted, they neither cite criminal statutes nor in any way describe any suspected criminal conduct. Clearly, such matters are set forth in the supporting Affidavits, but because those documents are neither attached to nor incorporated into the Warrant themselves, the information they provide does not "cure an otherwise defective search warrant." *Rosa,* 626 F.3d at 64. Under the settled Circuit law set forth above, failure to reference the suspected crimes would alone be enough to render the Warrants insufficiently particularized. *See 650 Fifth Ave.,* 830 F.3d at 99 ("for a warrant to meet the particularity requirement, it must identify the alleged crime for which evidence is sought"); *George*, 975 F.2d at 76 (warrant permitting search of evidence "relating to the commission of a crime" lacked particularity because "[n]othing on the face of the warrant tells the searching officer for what crime the search is being undertaken"); *see also United States v. Romain*, 678 Fed.Appx. 23, 25, 2017 WL 442175, at *1 (2d Cir. 2017) (Summary Order) ("[T]he government concedes that the warrant was facially deficient for failing to reference the criminal statutes that [defendant] was accused of violating even though the supporting document did contain that information.").

The Government argues, however, that explicit references to the crimes under investigation is unnecessary because the categories of documents subject to seizure make it "plain ... that this is a financial fraud case involving securities fraud in particular." Opp. at 28–29. That is unavailing for at least two reasons. First, the Government offers no authority, and the Court is aware of none, for the proposition that a warrant lacking an express reference to any crime or criminal conduct nonetheless satisfies the particularity requirement simply because the suspected crimes are arguably "inferable," Opp. at 29, from the warrant's remaining provisions. If anything, the Court of Appeals has rejected a similar argument, concluding in *George* that a warrant's inclusion of a list of seizable items that featured a McDonald's uniform, McDonald's management materials, a firearm, and a purse, did not mean that the otherwise "broad catch-all" phrase "any other evidence relating to the commission of ***a crime***" referred with particularity to a recent McDonald's robbery when "read in context." 975 F.2d at 74–76 (emphasis added).

***385** Second, the Government's factual premise is faulty. While it is true that the Warrants authorize seizure of categories of documents that conceivably could be consistent with an investigation into securities fraud, those categories

are sufficiently broad and numerous as to be consistent with an investigation into almost *any* form of financial crime (or even concealment of the fruits of some non-financial crime). *See e.g.,* NYGG Warrant Ex. A (making subject to seizure "financial records," "correspondence," "records of internal and external communications," shareholder and investor records, marketing materials, and documents reflecting corporate ownership or structure). Nothing about these categories would make it "plain" to a reader that securities fraud in particular was necessarily the subject of the search and limit the executing officers' discretion accordingly.[6]

The Government also urges that "no crime-identification requirement applies or should apply where ... (1) the subject warrant does not include a blanket permission to seize 'all evidence' or 'all documents' and (2) the categories of evidence to be seized are otherwise described with particularity." Opp. at 30. The binding case law in this Circuit simply reflects no such caveats, however, and, in any event and as explained further below, the items made subject to seizure in the Warrants are by no means "otherwise described with particularity." To the contrary, once the structure of the Warrants is taken into account, it is clear that their description of the items to be seized is essentially the functional equivalent of the very sort of "all-documents" authorization that, according to the Government, would make explicit reference to the crimes under investigation all the more important.

b. Expansive Categories of Generic Documents without Linkage to Suspected Criminal Conduct

The last point segues directly to the second reason why the Warrants are insufficiently particularized. Exhibit A to each of the Warrants sets forth expansive categories of often generic items subject to seizure—several of a "catch-all" variety —without, crucially, any linkage to the suspected criminal activity, or indeed any meaningful content-based parameter or other limiting principle. Importantly, the property listed is hardly, by "its particular character, contraband." See 2 Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* § 4.6(a) (5th ed. 2012). Rather, it is, from top to bottom, "the type of property" that is "generally in lawful use in substantial quantities," and, therefore, even "[g]reater care in description [i]s ... called for." *Id.* (also noting that "[a] more particular description than otherwise might be necessary is required when other objects of the same general classification are likely to be found at the particular place to be searched") (endnote citations omitted); *cf. United States v. Morisse,* 660 F.2d 132, 136 n.1 (5th Cir. 1981) (if the "nature of the [suspected illegal] activity does not allow for [the] ***386** ready segregation" of illegal items from "legal items," then "the "magistrate should take care to assure the warrant informs the law enforcement agent as to how he should distinguish between the illegal paraphernalia and the items that are held legally").

Specifically, Exhibit A authorizes seizure of, for example, the following buckets of material: "financial records," "notes," "memoranda," "records of internal and external communications," "correspondence," "audio tapes[ ] and video tapes," "photographs," "documents which may reflect the identifies of persons listed in Exhibit B or persons affiliated with the entities listed in Exhibit B," and others. *See, e.g.,* NYGG Warrant Ex. A. Several of these top-level categories are followed by sub-lists of more specific types of items, but, as the Government concedes, those do not purport to be in any way exhaustive or exclusionary and instead serve only an "illustrative" function. Opp. at 27. And, in any event, "even the most specific descriptions" on the sub-lists (e.g., "documents concerning or reflecting the movement of funds," "checks," "transaction records," "Rolodexes," "diaries," "calendars," etc.") are themselves "fairly general." *See United States v. Cardwell,* 680 F.2d 75, 78–79 (9th Cir. 1982); NYGG Warrant Ex. A.

Indeed, the only Warrant provisions that purport to place actual limitations or constraints of any sort on the executing officers' authority to seize items falling into these otherwise capacious buckets are those requiring that items to be seized "concern," "relate" to, or bear some similar generalized connection to at least one of the individuals and entities set forth in Exhibit B to the Warrants. The problem is that Exhibit B, as discussed, includes among its first few entries that very corporate entity (NYGG) whose premises was the subject of the first Warrant and Search and those very individuals (Benjamin and Michaela Wey) whose residence was the subject of the second. The result of that circular structure is that the would-be constraint imposed by Exhibit B is no constraint at all. Instead, the impact of the interplay between Exhibit A (the list of items to be seized) and Exhibit B (the list of relevant individual and entities) is that the Warrants broadly authorize the seizure from NYGG's offices of all "financial records," "notes," "memoranda," records of "communications," "correspondence," "tapes," "photographs," etc. *pertaining to NYGG itself.* So, too, they authorize seizure from the Wey Apartment of all such

materials *pertaining to the Weys themselves*. By the Warrants' terms, then, no connection to any suspected crime or to any other individual or entity listed on Exhibit B is necessary to render the expansive list of items set forth in Exhibit A seizable.

Lacking, accordingly, any practical tool to guide the searching agents in distinguishing meaningfully between materials of potential evidentiary value and those obviously devoid of it; the Warrants are—in function if not in form—general warrants. Indeed, insofar as any document located within a home or office at least arguably pertains in some way to the occupant or owner of the premises, the Court would struggle to conceive of any documents found within NYGG or the Wey Apartment that would *not* colorably fall within the scope of that authorization (and, as discussed further below, so too did the Government agents in charge of the Searches).

This deficiency, while concerning under any circumstances, is only exacerbated by the fact that the Warrants target, in significant measure, the contents of electronic devices, such as computers, internal and external hard drives, and smartphones. ***387** *See, e.g.,* NYGG Warrant Ex. A. As the Court of Appeals observed just days ago, especially given the practical risk that "every warrant for electronic information will become, in effect, a general warrant," a warrant that "lack[s] meaningful parameters on an otherwise limitless search of a defendant's electronic media"—including in its "fail[ure] to link the evidence sought to the criminal activity supported by probable cause"—does "not satisfy the particularity requirement." *Ulbricht,* 858 F.3d at 99–100 (internal quotation marks and alterations omitted) (quoting *Galpin,* 720 F.3d at 447; *Rosa,* 626 F.3d at 62)

In sum, the Warrants authorize the seizure of sweeping categories of materials, regardless of their potential connection (or lack thereof) to any suspected criminal activities and limited only by the requirement that they relate in some generalized way to the owner/occupant of the very premises subject to search. The conferral of such unfettered discretion on the executing officers, particularly in light of the Warrants' independent failure to identify any crime under investigation, is inconsistent with the Fourth Amendment's particularity requirement.[7]

c. Lack of Temporal Limitation

Finally, to the extent that lack of temporal limitation constitutes an independent factor militating against a determination of particularity, the Warrants undisputedly fail to limit the items subject to seizure by reference to any relevant timeframe or dates of interest. They do so despite the underlying Affidavits—and, ultimately, the Indictment—identifying timeframes, and often rather precise timeframes at that, for suspected criminal activity in relation to each of the Issuers purportedly implicated in Wey's suspected scheme. *See, e.g., United States v. Abboud,* 438 F.3d 554, 576 (6th Cir. 2006) (" 'Failure to limit broad descriptive terms by relevant dates, when such dates are available to the police, will render a warrant overbroad.' ") (quoting *United States v. Ford,* 184 F.3d 566, 576 (6th Cir. 1999)); *United States v. Kow,* 58 F.3d 423, 427 (9th Cir. 1995) (warrant "not sufficiently ***388** particular" in part because the "government did not limit the scope of the seizure to a time frame within which the suspected criminal activity took place"); *United States v. Abrams,* 615 F.2d 541, 545 (1st Cir. 1980) (deeming warrant insufficiently particularized and noting, among other things, that "[a] time frame should also have been incorporated into the warrant"); *United States v. Jacobson,* 4 F.Supp.3d 515, 526 (E.D.N.Y. 2014) ("a warrant's failure to include a temporal limitation on the things to be seized may, in certain circumstances, render a warrant insufficiently particular").

The Court recognizes that the "complexity and duration of the alleged criminal activities" discussed in the Affidavits may well make the Warrants' lack of a temporal limitation somewhat "less significant" of a factor in determining their constitutional sufficiency than it otherwise might be. *See Hernandez,* 2010 WL 26544, at *11. Still, the "absence of such a limit reinforces the Court's conclusion" that the Warrants are insufficiently particularized. *Zemlyansky,* 945 F.Supp.2d at 459–60; *Vilar,* 2007 WL 1075041, at *23 (the "lack of particularity is only compounded by the absence of any date restriction on the items to be seized"); *United States v. Triumph Capital Grp., Inc.,* 211 F.R.D. 31, 58 (D. Conn. 2002) (recognizing a "temporal limitation" as "one indicia of particularity").

d. The All–Records Exception Does Not Save the Warrants From Their Lack of Particularity

The Government contends that, even if the Warrants lack particularity, they fall within the so-called "all-records exception" and thus do not run afoul of the Fourth Amendment. Opp. at 36–37. The Court concludes otherwise.

i. Legal Standard for the All–Records Exception

Courts in the Second Circuit have recognized that "[w]hen there is probable cause to believe that an entire business is 'pervaded' or 'permeated' with fraud, seizure of all records of the business is appropriate, and broad language used in a search warrant will not offend the particularity requirement." *United States v. D'Amico,* 734 F.Supp.2d 321, 360 (S.D.N.Y. 2010). Under those limited circumstances, "broad language used in warrants will not offend the particular requirements." *U.S. Postal Serv. v. C.E.C. Servs.,* 869 F.2d 184, 187 (2d Cir. 1989). This principle is commonly referred to as the "all-records exception to the particularity requirement." *D'Amico,* 734 F.Supp.2d at 360 (internal quotation marks omitted) (citing *United States v. Burke,* 718 F.Supp. 1130, 1139 (S.D.N.Y. 1989)); *see also United States v. Smith,* 05–cr–293A, 2007 WL 2088938, at *3 (W.D.N.Y. Jul. 19, 2007) ("Although the particularity requirement of the Fourth Amendment creates a general presumption against 'general' or 'all-records' warrants, courts, including the Second Circuit, have recognized an exception where there is probable cause to believe that criminal activity permeates the business to be searched."). From a strictly analytical perspective, however, "it is not so much an 'exception' to the particularity requirement ... as a recognition that a warrant—no matter how broad—is, nonetheless, legitimate if its scope does not exceed the probable cause upon which it is based." *United States v. Bowen,* 689 F.Supp.2d 675, 683 n.6 (S.D.N.Y. 2010) (internal quotation marks omitted); *cf. Hickey,* 16 F.Supp.2d at 241 ("The more extensive the probable wrongdoing, the greater the permissible breadth of the warrant.").

For the all-records exception to apply, the affidavit in support of the ***389** search warrant need not necessarily lay out "specific factual evidence demonstrating that every part of the enterprise in question is engaged in fraud"; rather, it must only set forth "sufficient factual evidence of fraudulent activity from which a magistrate could infer that those activities are 'just the tip of the iceberg.' " *Burke,* 718 F.Supp. at 1139–40 (additional internal quotation marks omitted) (quoting *United States v. Offices Known as 50 State Distrib. Co.,* 708 F.2d 1371, 1375 (9th Cir. 1983)). Still, "[t]he Fourth Amendment requires more than mere extrapolation to activate the [all-records] principle." *Hickey,* 16 F.Supp.2d at 241. And courts assessing the applicability of the exception must satisfy themselves that "the Government ... provided the magistrate judge with sufficient probable cause to believe that the *entire* business operation is a scam." *Zemlyansky,* 945 F.Supp.2d at 461 (internal quotation marks and alterations omitted) (emphasis in original); *United States v. Paccione,* 738 F.Supp. 691, 708 (S.D.N.Y. 1990) ("Courts have consistently held that where a business is *totally illegal,* a search warrant may properly authorize the seizure of all documents of the business.") (emphasis added).

ii. The All–Records Exception Does Not Apply Here

First, a preliminary observation: while the probable cause showing necessary to invoke the all-records exception is always substantial, the Government faces an even higher hurdle than usual in attempting to apply it to the Apartment Warrant. Indeed, as several Circuits have recognized, "it would require extraordinary proof to demonstrate that an individual's entire life is consumed by fraud and that *all* records found in the home were subject to seizure." *United States v. Falon,* 959 F.2d 1143, 1148 (1st Cir. 1992); *United States v. Humphrey,* 104 F.3d 65, 69 n.2 (5th Cir. 1997) ("the issuance of all records searches of homes" will be upheld "only in extreme cases"); *see also United States v. Cherna,* 184 F.3d 403, 409 (5th Cir. 1999) ("[I]it is more difficult to demonstrate probable cause for an 'all records' search of a residence than for other searches."). For that reason, even "when an individual's allegedly fraudulent business activities are centered in his home," the " 'all records' doctrine must be applied with caution" in the context of a home search, and, absent "unusual proof," any "broad categories of items ... must be sufficiently linked to the alleged criminal activity so as to distinguish them from innocent personal materials." *Falon,* 959 F.2d at 1148; *see also United States v. Ostrowski,* 822 F.Supp.2d 66, 71 (D. Mass. 2011) ("[E]ven pervasive fraud cannot justify seizure of every record from an individual's home."). While the Second Circuit does not appear to have addressed this issue directly, its decisions on the subject strongly signal that the all-records exception is generally limited to the seizure of "*business* records" and applicable only when there is probable cause to believe that a "*business* was permeated with fraud." *Nat'l City Trading Corp. v. United States,* 635 F.2d 1020, 1026 (2d Cir. 1980) (emphasis added); *C.E.C. Servs.,* 869 F.2d at 187 (same).

Even assuming, however, that the all-records exceptions could conceivably save both the NYGG Warrant and the Apartment Warrant, the Court finds that both Warrant applications fell short of providing Magistrate Judge Dolinger with "sufficient probable cause to believe that [Wey's]

entire business operation [was] a scam." *Zemlyansky,* 945 F.Supp.2d at 461 (internal quotation marks and alterations omitted) (emphasis in original); *see also D'Amico,* 734 F.Supp.2d at 360 (all-records doctrine applies where "there is probable cause to believe that an entire business is ***390** 'pervaded' or 'permeated' with fraud"). As noted above, the Komar Affidavit—and, by extension, the Garwood Affidavit—described NYGG, in terms suggesting some measure of presumed legitimacy, as a "corporate advisory firm" with a "special[ty]" in "introducing middle-market Chinese operating companies to the U.S. capital markets." *See, e.g.,* Komar Aff. ¶ 16. Accounting for all of the substantial evidence marshalled across the Komar Affidavit's nearly 100 pages, it connected NYGG and Wey to a scheme implicating, at most, five or six discrete deals involving specifically identified Issuers, with the alleged misconduct pertaining to each company occurring in some at least roughly defined timeframe. *See* Reply Memorandum of Law in Further Support of Defendant Benjamin Wey's Motion to Suppress, To Dismiss the Indictment, and For Other Relief, Dkt. No. 62 ("Reply"), at 19–20. The Komar Affidavit did not set forth any evidence, explicit or implicit, that the scheme either constituted just the "tip of iceberg" with respect to fraudulent activity involving NYGG or the Wey Apartment, or that the scheme itself constituted the entirety—or even a substantial portion—of NYGG's or Wey's overall business operations. It made no showing, for example, that NYGG was merely a front for the scheme or that the scheme infused or was otherwise "inseparable" from the balance of NYGG's corporate advisory activities. *Burke,* 718 F.Supp. at 1141. Nowhere, more generally, did it suggest that NYGG was a so-called "boiler room" operation or similar sham enterprise. *Id.* at 1140–41.

Indeed, the Komar Affidavit, as the Government concedes, "candidly acknowledged," Opp. at 36, that there were "legitimate aspects of [NYGG's] business," Komar Aff. ¶ 35(b) n.11, but it made no effort to characterize the scope of the suspected fraud relative to NYGG's apparently above-board operations. *See Zemlyansky,* 945 F.Supp.2d at 463 ("The affidavit offers no information about the size or scope of [the subject] business, its clients, whether only part of the office deals with the kind of billing at issue in the alleged scheme, [or] the manner in which or degree to which it is controlled by the [relevant] scheme...."). To the contrary, Komar admitted that he lacked the necessary information to do so, averring that the NYGG Search would help provide the FBI with "background" information to better understand the "scope" of the suspected fraudulent scheme as "compared to [NYGG's] overall business." Komar Aff. ¶ 35(b) n.11.

True, the fact that a business "engaged in *some* legitimate activity" may not necessarily "defeat the all-records exception" on its own. *D'Amico,* 734 F.Supp.2d at 360 (emphasis in original). Thus, for example, an enterprise demonstrated by the FBI to have been specifically created to serve as a front to launder organized crime proceeds could not invalidate an expressly approved all-records application by pointing to some potentially legitimate sales activity on the side. *Id.* at 356–62. But clear acknowledgment, of the sort offered by Komar, that an affiant is essentially in the dark as to how a suspected fraud fits into a broader "legitimate" business is inconsistent with a demonstration of probable cause that the fraud entirely permeates the enterprise.

In fact, the Komar Affidavit recognized the relative narrowness of its actual probable cause showing, consistently asserting, for example, that there was probable cause to believe that "documents and other evidence *relating to the SmartHeat, Deer, and AgFeed schemes*" would be found at the NYGG offices. Komar Aff. ¶ 35; *see also id.* ¶ 38 ("There [is] probable cause to believe that the [NYGG offices] currently contain evidence *of Wey's use of nominees to conceal his ownership in CleanTech and Nova Lifestyle.*") (emphasis added); ***391** *see also Burke,* 718 F.Supp. at 1141 (rejecting all-records argument pertaining to art gallery in part because the affidavit itself made clear that there was "probable cause to believe that mail fraud and wire fraud *involving the sale of purported fine art prints by Salvador Dali,* had been committed" by the subject gallery) (emphasis in original) (internal quotation marks and alterations omitted).

The Garwood Affidavit, for its part, fell especially short of making the heightened showing required to authorize the seizure of all records from the Wey Apartment. Even incorporating as it did the Komar Affidavit, the Garwood Affidavit nowhere approached a "demonstrat[ion]" from which one could draw the reasonable inference that Wey's "entire life [was] consumed by fraud." *Falon,* 959 F.2d at 1148. Nor did it aver that NYGG's allegedly fraudulent business activities were in any way "centered" on the Wey Apartment, *id.,* or that there "was considerable overlap between [Wey's] personal and business lives," *Cherna,* 184 F.3d at 409 (citing *Humphrey,* 104 F.3d at 68–69). To the contrary, the Garwood Affidavit's probable cause showing as to the Wey Apartment itself was, all things considered, relatively narrow, focusing principally on allegations that: (i)

Michaela Wey often performed "bookkeeping" and "payroll" functions for NYGG from the Wey Apartment, where she "sometimes mail[ed] checks"; (ii) Deer stock certificates had been sent to the Wey Apartment in April 2009; and (iii) Wey's sister had purportedly executed suspicious electronic fund transfers to personal accounts in the name of Michaela Wey. Garwood Aff. ¶¶ 6–12. Such a showing might well justify the seizure of materials pertaining to the purported scheme outlined in the Komar Affidavit, but it most assuredly did not rise to the level of supporting an all-records authorization.

Further belying the suggestion that the all-records exception excuses the Warrants' lack of particularity, the evidence before the Court indicates that the Government neither intended to seek formal authority to seize all records from NYGG and/or the Wey Apartment nor understood itself at any time—until perhaps it joined issue on the instant motion—to be in possession of any such authority. The Komar and Garwood Affidavits nowhere made the explicit assertion that NYGG—or any other Wey-linked business operation for that matter—was permeated by fraud. They also did not explicitly request permission to execute an all-records seizure. *See, e.g., Vilar,* 2007 WL 1075041, *21 ("[T]he Affidavit itself makes no explicit allegation that the [subject] entities were permeated with fraud."). Moreover, apart from AUSA Massey's somewhat rote incantations on direct examination at the Hearing that NYGG was "permeated with fraud" at the time of the Searches, Hearing Tr. 13:10–15—assertions that the Court found too rehearsed to be persuasive[8]—the Government's witnesses testified across the board that the Warrants covered something less than all records from either location (although, as discussed further below, they also struggled to articulate any limiting principle) and they had no recollection of actually applying for all-records authorization. *See, e.g., id.* 47:4–8 (**Q.** "Is it fair to say, sir, that Exhibit A was an attempt by you to cover basically every form or format of material that could be found in a location from notes, handwritten notes, scraps of paper, every form of item that could be found?" **A.** "No, that's not correct.") ***392** (Massey); *id.* 33:5–8 (**Q.** "What I'm trying to figure out from your testimony, sir, is whether you are testifying that you actually made the [Warrant] application pursuant to the [all-records] doctrine or not?" **A.** "I don't recall. I simply don't recall."); *id.* 188:16–18 (**Q.** "Never occurred to you that [the NYGG Warrant] might be a warrant that covered everything in the office?" **A.** "I don't feel it covered everything in the office.") (Komar); *see also id.* 40:4–10 (**Q**: "... do you believe that your understanding of the business gave you the right to seize every record at the home of Benjamin and Michaela Wey?" **A.** "No.") (Massey). As several courts outside this Circuit have recognized, "if the [G]overnment is relying upon the 'permeated with fraud' exception to support an application for an otherwise overly-broad search warrant, it should state so in the application rather than attempting a post-hoc rationalization." *United States v. Bridges,* 344 F.3d 1010, 1020 (9th Cir. 2003) (Thomas, J., concurring in pertinent part); *cf. Abrams,* 615 F.2d at 544 ("If, as the government urges, the affidavit information called for all ... of the Medicare-Medicaid records in the offices, then the warrant should have said so."); *United States v. Winn,* 79 F.Supp.3d 904, 920 (S.D. Ill. 2015) ("The bottom line is that if [the applying officer] wants to seize every type of data from the cell phone, then it was incumbent upon him to explain in the complaint how and why each type of data was connected to [Defendant's] criminal activity, and he did not do so.").

In all of these ways, the circumstances here are readily distinguishable from those presented in *D'Amico,* the case on which the Government relies to advance its all-records argument. Opp. at 36–37. There, the FBI not only expressly sought permission to seize "all documents relating to" the business to be searched, but it also established in its warrant application that the subject business, while perhaps engaging in some attempt to sell energy drinks as a side operation, had specifically been created to, and did, serve primarily as a front for the laundering of proceeds generated by illicit mafia operations. 734 F.Supp.2d at 356–62. For that matter, the circumstances here differ more generally from the typical cases in which the all-records exception is applied in this Circuit: those "involv[ing] rampant misconduct and little, if any, legitimate business activities." *Vilar,* 2007 WL 1075041, at *21 (collecting cases); *see also Zemlyansky,* 945 F.Supp.2d at 461 ("In cases where the all records exception has been applied, the affidavit submitted in support of the warrant contained detailed information that would provide reason to believe that all or nearly all of the business under investigation was illegal."); *Burke,* 718 F.Supp. at 1139–1140 (surveying case law and noting that evidence sufficient to invoke all-records exception tends to "consist of a large number of fraudulent transaction or of documentation—in the form of information gleaned from interviews with former employees or from undercover surveillance of the operation—that the entire operation is a scam").

More instructive here are cases like *Hickey* and *Burke.* In *Hickey,* four corporations were allegedly involved in a RICO, fraud, and money laundering scheme centered on controlling and exploiting commercial garbage operations in the Town of

Islip, New York (the "Islip fraud"). 16 F.Supp.2d at 226. Law enforcement agents obtained warrants to seize "all business records" of each of the four entities. *Id.* at 237. The court invalidated the warrants, concluding as pertinent here that they were not salvageable under the all-records exception because the warrant application's probable cause showing focused on ***393** the "core criminality" targeted by the investigation—the "one overriding scheme" represented by the Islip fraud—and lacked sufficient information to suggest that the "other operations of the defendant corporations" were "similarly corrupted." *Id.* at 240–241. And in *Burke,* the court refused to apply the all-records exception to warrants to search offices of Barclay Galleries, even though the underlying affidavits identified six fraudulent transactions involving Salvador Dali prints and several related fraudulent statements and misrepresentations, and averred, based on information from confidential sources, that the offices housed a "a boiler room operation." 718 F.Supp. at 1138–40. Judge Mukasey observed that "[n]otably absent" from the affidavits was "any indication that the government believed ... that Barclay's sale of non-Dali artwork was also fraudulent or that Barclay's sale of fraudulent Dali artwork represented just a sample of its pervasively fraudulent sales," and that the Government made no "showing that the sale of Dali prints was inseparable from the sale of print by other painters." *Id.* at 1140–41.

The instant facts are analogous. The Komar and Garwood Affidavits unquestionably establish probable cause to search for and seize *something*: for example, materials pertaining to the specific entities and individuals purportedly implicated as Issuers or Nominees in the five to six transactions on which the Affidavits focused. They fall short, however, of establishing the requisite probable cause to believe that Wey's entire business operation was a scam, so as to justify the seizure of all records from either NYGG or the Wey Apartment.

For the foregoing reasons, the Court concludes that both Warrants lack particularity and that shortcoming is not excused under the all-records exception.

2. The Search Warrants Are Overbroad

As noted above, "breadth and particularity are related but distinct concepts." *Ulbricht,* 858 F.3d at 102. The former issue is "whether the items listed as 'to be seized' in the warrant were overboard because they lacked probable cause" and the second is "whether the warrant was sufficiently particularized on its face to provide the necessary guidelines for the search by the executing officers." *Hernandez,* 2010 WL 26544, at *7 (citations omitted); *see also Cohan,* 628 F.Supp.2d at 359 ("A warrant ... can be unconstitutionally infirm in two conceptually distinct but related ways: either by seeking specific material as to which no probable cause exists, or by giving so vague a description of the material sought as to impose no meaningful boundaries."). For many of the same reasons set forth above, the NYGG Warrant and the Apartment Warrant are constitutionally overbroad. Specifically, owing in large measure to their failure to impart meaningful guidelines to the searching agents (a particularity problem), the Warrants purport to authorize the seizure of, essentially, all documents from NYGG and the Wey Apartment. As demonstrated in the foregoing discussion of the all-records exception, however, such authorization exceeds the scope of the probable cause showing submitted to the Magistrate Judge. That is an independent (if related) overbreadth problem.

The Court is, of course, mindful of the deference generally owed to a magistrate's probable cause determinations, and it has no doubt that Magistrate Judge Dolinger was correct insofar as he found probable cause to believe that some subset of the materials likely located within the NYGG offices and the Wey Apartment could constitute evidence of criminal activity. But the sheer scope of the Warrants—reaching, ***394** as shown above, essentially all documents pertaining to NYGG and/or the Weys unlimited by relevance to criminal conduct or by timeframe—precludes a finding that the seizure authorization remained within the bounds of the Government's probable cause showing. The Court cannot agree, to take but a few straightforward examples, that the Affidavits support the sweeping seizure of all "notes" "relating to" NYGG, or all "correspondence" and "photographs" "concerning" either one of the Weys. *See* NYGG Warrant Exs. A–B; Apartment Warrant Exs. A–B. Simply put, the Warrants are, in essence, all-records warrants unsupported by probable cause to seize all records. That constitutes a violation of the Fourth Amendment.

C. The Good Faith Exception Does Not Save the Searches

The Government argues strenuously that, even assuming the Warrants are constitutionally deficient, the good faith exception properly applies to the execution of both Searches, thus precluding suppression of the Search fruits. Opp. at 38–41; Supplemental Memorandum of Law in Opposition to

Defendant's Motion to Suppress Evidence, Dkt. 86 ("Gov't Supp. Opp."), at 13–17. For the following reasons, and based on its factual findings following the two-day Hearing, the Court rejects this argument.

1. Background Law on the Exclusionary Rule and the Good Faith Exception

The Fourth Amendment "contains no provision expressly precluding the use of evidence obtained in violations of its commands." *Arizona v. Evans*, 514 U.S. 1, 10, 115 S.Ct. 1185, 131 L.Ed.2d 34 (1995). Nevertheless, the Supreme Court has "establish[ed] an exclusionary rule that, when applicable, forbids the use of improperly obtained evidence at trial." *Herring v. United States,* 555 U.S. 135, 139, 129 S.Ct. 695, 172 L.Ed.2d 496 (2009). "[T]his judicially created rule is 'designed to safeguard Fourth Amendment rights generally through its deterrent effect.' " *Id.* at 139–40, 129 S.Ct. 695 (quoting *United States v. Calandra,* 414 U.S. 338, 348, 94 S.Ct. 613, 38 L.Ed.2d 561 (1974)).

Still, "[t]he fact that a Fourth Amendment violation occurred —*i.e.,* that a search or arrest was unreasonable—does not necessarily mean that the exclusionary rules applies." *Id.* at 140, 129 S.Ct. 695. To the contrary, the Supreme Court has repeatedly noted that "exclusion 'has always been our last resort, not our first impulse.' " *Id.* (quoting *Hudson v. Michigan,* 547 U.S. 586, 591, 126 S.Ct. 2159, 165 L.Ed.2d 56 (2006)). In keeping with that admonition, the Supreme Court has recognized several "important principles that constrain application of the exclusionary rule." *Id.* "First, the exclusionary rule is not an individual right and applies only where it 'results in appreciable deterrence' " of "Fourth Amendment violations in the future." *Id.* at 141, 129 S.Ct. 695 (additional internal quotation marks and brackets omitted) (quoting *Leon*, 468 U.S. at 909, 104 S.Ct. 3405); *see also Raymonda,* 780 F.3d at 117 ("Neither a personal constitutional right nor a means to redress the injury of an unconstitutional search, the exclusionary rule is designed to deter future Fourth Amendment violations.") (internal quotation marks omitted). And second, "the benefits of deterrence" must "outweigh" the often "substantial social costs" of "letting guilty and possibly dangerous defendants go free." *Herring,* 555 U.S. at 141, 129 S.Ct. 695 (internal quotation marks and citations omitted); *see also Pa. Bd. of Probation & Parole v. Scott,* 524 U.S. 357, 364–65, 118 S.Ct. 2014, 141 L.Ed.2d 344 (1998) (the exclusionary rule's "costly toll upon truth-seeking and law ***395** enforcement objectives presents a high obstacles for those urging application of rule") (internal quotation marks omitted). Thus, in order "[t]o trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Herring,* 555 U.S. at 144, 129 S.Ct. 695. Such deterrence interests are most often implicated by "deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Id.* Conversely, when police conduct "involves only simple, isolated negligence, exclusion simply cannot pay its way." *Raymonda,* 780 F.3d at 118 (internal quotation marks omitted).

The so-called "good faith exception" to the exclusionary rule embodies these principles. That doctrine provides that "evidence obtained by officers in objectively reasonable reliance on a warrant subsequently invalidated by a reviewing court is not generally subject to exclusion." *Id.* (internal quotation marks omitted). "Likewise government agents act in good faith when they perform 'searches conducted in objectively reasonable reliance on binding appellate precedent.' " *Ganias,* 824 F.3d at 236 (quoting *Davis v. United States,* 564 U.S. 229, 232, 131 S.Ct. 2419, 180 L.Ed.2d 285 (2011)). Lest there be any doubt on the matter, the Second Circuit has recently admonished that "such reliance" must actually be "*objectively reasonable.*" *Id.* at 221 (emphasis in original). That requirement generally demands "that the officer exhibit 'reasonable knowledge of what the law prohibits.' " *Raymonda,* 780 F.3d at 119 (quoting *George,* 975 F.2d at 77); *see also Leon*, 468 U.S. at 919, 104 S.Ct. 3405 (" 'evidence obtained from a search should be suppressed only if ... the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional' ") (quoting *United States v. Peltier,* 422 U.S. 531, 95 S.Ct. 2313, 45 L.Ed.2d 374 (1975)). And the " 'inquiry is confined to the objectively ascertainable question whether a reasonably well trained office would have known that the search was illegal' in light of 'all the circumstances.' " *Herring,* 555 U.S. at 145, 129 S.Ct. 695 (quoting *Leon,* 468 U.S. at 922 n.23, 104 S.Ct. 3405).[9]

As a corollary of sorts to the objective reasonableness requirement, the good faith exception "cannot shield even an officer who relies on a duly issued warrant in at least four circumstances: '(1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance

upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable.' " *Raymonda,* 780 F.3d at 118 (quoting *United States v. Clark,* 638 F.3d 89, 100 (2d Cir. 2011)); *see also George,* 975 F.2d at 77 ("[r]easonable reliance does not allow an officer to conduct a search with complete disregard of the warrant's validity because the standard of reasonableness is an objective one") (internal quotation marks and alterations omitted).

" 'The burden is on the government to demonstrate the objective reasonableness of the officers' good faith reliance' on an ***396** invalidated warrant." *Clark,* 638 F.3d at 100 (quoting *George,* 975 F.2d at 77).

2. Background Law on the Good Faith Exception in the Context of Insufficiently Particularized Warrants

The Supreme Court has long recognized that " 'a warrant may be so facially deficient—*i.e.,* in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid.' " *Groh,* 540 U.S. at 565, 124 S.Ct. 1284 (quoting *Leon*, 468 U.S. at 923, 104 S.Ct. 3405). In *Groh,* the Supreme Court had occasion, in the context of a *Bivens* action, to apply that admonition.

Specifically, the *Groh* Court considered whether a federal agent was entitled to qualified immunity despite having executed a search warrant that was facially deficient for lacking a particularized description—or indeed any description at all—of the items to be seized. 540 U.S. at 557–65, 124 S.Ct. 1284. After noting that the "the same standard of objective reasonableness that [is] applied in the context of a suppression hearing ... defines the qualified immunity accorded an officer," the *Groh* Court answered in the negative, concluding that "[g]iven that the particularity requirement is set forth in the text of the Constitution, no reasonable officer could believe that a warrant that plainly did not comply with that requirement was valid." *Id.* & n.8 (internal quotation marks and citation omitted). Notably, and as discussed above, the *Groh* Court reached that conclusion after rejecting the defendant officer's argument that "the goals served by the particularity requirement" had been "otherwise satisfied" by particularized (but unincorporated) warrant application papers and by the agent's own "restraint" in keeping the "scope" of the ultimate "search [from] exceeding the limits set forth in the application." *Id.* at 557–62, 124 S.Ct. 1284.[10]

Six years later, in *Rosa,* the Second Circuit recognized that *Groh* had "disallow[ed] consideration of unattached and unincorporated supporting documents to cure an otherwise defective search warrant," and accordingly deemed the warrant in question insufficiently particularized on its face —notwithstanding that it had issued on the strength of a more detailed (but unincorporated) affidavit—because it "fail[ed] to link the items to be searched and seized to the suspected criminal activity." 626 F.3d at 58–59, 62–64 (2d Cir. 2010) (also noting that the warrant was "overbroad and provided the officers with no judicial limit on the scope of their search" and, accordingly, "fail[ed] for lack of particularity"). Nevertheless, the *Rosa* Court held that the good faith exception saved the fruits of the search from exclusion. *Id.* at 64–66. Citing the deterrence and culpability principles highlighted by the Supreme Court in its then-recent *Herring* decision (and discussed above), the Second Circuit concluded—on what has aptly been described as the "highly unusual facts"[11] of the *Rosa* case—that even though the officers executed a warrant that on its face did not comply with the Fourth Amendment's particularity requirement, there was "nothing to suggest deliberateness and culpability on the [their] part," that ***397** they "acted reasonably" under the circumstances, and that the exclusionary rule would thus "serve little deterrent purpose" moving forward. *Id.*

In support of that determination, the *Rosa* Court pointed to several fact-specific considerations: (i) that the warrant application, issuance, and execution had all occurred under intense "time pressures" in "the three hours from 2:00 to 5:00 am" of a single morning; (ii) that the application's affiant led the execution team and was later responsible for searching recovered digital media; (iii) that there was "no evidence that ... [the] officers actually relied on the defective warrant, as opposed to their knowledge of the investigation and the contemplated limits of the town justice's authorization, in executing the search"; and (iv) that there was "no evidence that the team of officers searched for, or seized, any items that were unrelated to the crimes for which probable cause had been shown" in the application. *Id.* Emphasizing repeatedly that it operated "[u]nder the facts" and the "circumstances of th[is] case" and that "application of the exclusionary rule will vary in accordance with the facts of each case," the Court found the "requisite levels of deliberateness and culpability justifying suppression" to be "lacking." *Id.*

In *Zemlyansky,* a district court opinion issued three years after *Rosa,* Judge Oetken engaged in a thoughtful and

persuasive synthesis of the *Groh, Herring,* and *Rosa* decisions. Ultimately, *Zemlyansky* concluded, "the culpability standards and deterrence considerations that form the heart of *Herring's* good faith inquiry will ordinarily, though not always, be satisfied where a police officer acted in an objectively unreasonable manner by violating clearly established Fourth Amendment law," but there are at least "some circumstances" in which "there will be daylight between (1) a finding that an officer acted in an objectively unreasonable manner and (2) a finding that the deterrence and culpability concerns identified in *Herring* weigh in favor of suppression." 945 F.Supp.2d at 469–70 (also cautioning that "these factors will likely align in the vast majority of cases where the applicable Fourth Amendment law is clearly established"). Accordingly, in Judge Oetken's view, "courts must independently test each requirement before suppressing." *Id.* at 469. That is, the "Court must first consider whether the officers in this case acted in an objectively reasonable manner. If the answer to that question is no, and if the officers violated clearly established law, then the Court must determine whether the officers nonetheless fall into the narrow gap described in *Rosa* between violations of clearly established law and circumstances where an officer's conduct nonetheless constituted isolated negligence." *Id.* at 472.

This Court finds the *Zemlyansky* framework to be consistent with the repeated signals from the Court of Appeals in recent years that objective unreasonableness and deterrence value are independent (though related) factors to be considered separately, and that the absence of either one may suffice to bring police conduct within the good faith exception. *See, e.g., Ganias,* 824 F.3d at 236–37 (exclusionary rule will not apply if government agents acted in "objectively reasonable good faith reliance" on a warrant or binding appellate precedent or if the "benefits of deterring the Government's unlawful actions" do not "appreciably outweigh" the costs of suppression); *see also Romain,* 678 Fed.Appx. at 24–27, 2017 WL 442175, at *1–2. Accordingly, the Court will apply that framework here.

3. There Could Be No Objectively Reasonable Reliance on the Facially Unparticularized Warrants

As the Supreme Court has made clear, the objective reasonableness standard in ***398** the context of the good faith exception is "the same" as that applicable to assessments of qualified immunity. *Groh,* 540 U.S. at 565 n.8, 124 S.Ct. 1284 (quoting *Malley v. Briggs,* 475 U.S. 335, 344, 106 S.Ct. 1092, 89 L.Ed.2d 271 (1986)). In turn, "[w]hether an official protected by qualified immunity may be held personally liable for an allegedly unlawful action" generally depends "on the objective legal reasonableness of the action, assessed in light of the legal rules that were clearly established at the time it was taken." *Messerschmidt v. Millender,* 565 U.S. 535, 546, 132 S.Ct. 1235, 182 L.Ed.2d 47 (2012) (internal quotation marks and alterations omitted) (quoting *Anderson v. Creighton,* 483 U.S. 635, 639, 107 S.Ct. 3034, 97 L.Ed.2d 523 (1987)).

As set forth above, the NYGG Warrant and the Apartment Warrant both on their face plainly violate multiple components of the Fourth Amendment's particularity requirement as construed by the Supreme Court and the Second Circuit. At a minimum, neither identifies in any way the crimes under investigation. And both authorize the seizure of multiple expansive categories of records (e.g., "notes," "memoranda," "correspondence," "communications," "photographs," etc.) without any meaningful linkage to the suspected criminal conduct and limited only, at the outer boundaries, to some relationship to the owner/occupant of the premises being searched. Each of these deficiencies runs afoul of principles that had already been clearly established in binding precedents when the Warrants were issued and Searches conducted. *See, e.g., George,* 975 F.2d at 76 (2d Cir. 1992) (no identification of crimes); *Bianco,* 998 F.2d at 1115–16 ("highly generalized" and "broad" categories of documents not "tied to particular crimes" or subject to "more particular limiting language"); *Buck,* 813 F.2d at 590–93 & n.2 ("catch-all" descriptions of categories of items to be seized without meaningful limiting language); *Rosa,* 626 F.3d at 62; (lack of linkage to suspected criminal activity or other meaningful parameters on search); *see also Zemlyansky,* 945 F.Supp.2d at 472 (collecting pre-2012 cases); *Vilar,* 2007 WL 1075041, at *22 (same). Both the Supreme Court and the Second Circuit had already made abundantly clear, moreover, that such deficiencies could not be cured by the unincorporated, unattached Komar and Garwood Affidavits. *See Groh,* 540 U.S. at 557–58, 124 S.Ct. 1284; *Rosa,* 626 F.3d at 62–64. Finally, and as discussed further below, the record reflects no evidence that the agents' failure to recognize these infirmities may be attributed to exigent or otherwise unusual circumstances that existed when the Affidavits or the Warrants were drafted or the Searches conducted. *Cf. Groh,* 540 U.S. at 565 n.9, 124 S.Ct. 1284 ("[P]etitioner does not contend that any sort of exigency existed when he drafted the affidavit, the warrant application, and the warrant, or when he conducted the search. This is

not the situation, therefore, in which we have recognized that 'officers in the dangerous and difficult process of making arrests and executing search warrants' require 'some latitude.' ") (quoting *Maryland v. Garrison,* 480 U.S. 79, 87, 107 S.Ct. 1013, 94 L.Ed.2d 72 (1987)).

To be sure, when an "alleged Fourth Amendment violation involves a search or seizure pursuant to a warrant, the fact that a neutral magistrate has issued a warrant is the clearest indication that the officers acted in an objectively reasonable manner." *Messerschmidt,* 565 U.S. at 546, 132 S.Ct. 1235. But the mere presence of a warrant "does not end the inquiry into objective reasonableness." *Id.* at 547, 132 S.Ct. 1235. When, as here, a warrant plainly ***399** fails to comport with well-settled particularity requirements, officers' reliance upon it—especially in the absence of a credible circumstance-specific explanation—can hardly be deemed objectively reasonable. *See, e.g., George,* 975 F.2d at 78 ("in light of the settled nature of the law concerning the failure for lack of particularity of warrants authorizing the search for 'evidence' limited only by reference to 'a crime,' " the subject warrant was "the type of facially invalid warrant that could not have been relied upon in good faith because one who simply looked at the warrant would suspect it was invalid") (internal quotation marks, alterations, and citation omitted); *Hickey,* 16 F.Supp.2d at 244 (executing officers could not reasonably rely on warrants that were so lacking in particularity as to be "general in nature"); *United States v. One Parcel of Prop. Located at 18 Perkins Road, Woodbridge, Conn.,* 774 F.Supp. 699, 707 (D. Conn. 1991) ("Courts commonly refuse to find good faith reliance when the warrant is too broadly worded or its terms so vague or unspecific that it fails to distinguish adequately between items that are evidence of a crime and innocent possessions.") (internal quotation marks and brackets omitted).[12]

4. Culpability in Execution and Deterrence Considerations Weigh in Favor of Suppression

a. The *Rosa* Factors

The Court next considers the impact of the factors highlighted in *Rosa.* Specifically, it asks whether those factors operate here to render the officers' conduct in applying for or executing the Warrants insufficiently culpable for suppression to carry meaningful deterrence benefits or otherwise support a finding that any such benefits would not be worth the " 'price paid by the justice system.' " *Rosa,* 626 F.3d at 64 (quoting *Herring,* 555 U.S. at 144, 129 S.Ct. 695). In light of its factual findings and for the reasons set forth below, the Court concludes that they do not.

i. Exigency

As alluded to above, exigency, arguably the most critical *Rosa* factor, is entirely absent from this case. *See Rosa,* 626 F.3d at 64–66 (repeatedly citing the "time pressures" under which the warrant was obtained and executed and the "necessary speed" with which the officers acted in the "three hours from 2:00 am to 5:00 am"). Indeed, in stark contrast to *Rosa,* there is no dispute here that AUSA Massey and Agent Komar had been leading an investigation into NYGG and Wey for a substantial period of time prior to the Searches and prepared the NYGG Warrant application over the course of "weeks," if not "months." Hearing Tr. 30:23–31:4. Agent Komar conceded that once the NYGG Warrant issued, the FBI had a 10–day window in which to execute it—10 days in which, for example, all members of the NYGG Search team could have reviewed the Komar Affidavit—but it chose, for reasons not clear from the record, to proceed the following day. *Id.* 186:3–25.

In addition, the Searches themselves were not constrained by lack of time or resources. To the contrary, each Search lasted between four and five hours (with every indication that even more time could have been taken, if necessary), each Search was conducted by a team of some seventeen to twenty FBI agents, and, as Government witnesses noted at the Hearing, ***400** neither Search team had to contend with a "substantial" volume of hard-copy materials found onsite. *See supra* Sections I.D.1.–3. Agent Komar testified that the NYGG Search team had more than enough time to review every single hard-copy document found in the NYGG offices onsite. Hearing Tr. 133:14–134:13. Following the physical Searches, moreover, FBI personnel evinced no particular hurry about reviewing the recovered electronic evidence; as discussed, comprehensive pertinence review of that material did not begin for almost a year and half. *See supra* Section I.D.4.

Under these circumstances, the Court finds, as a factual matter, that the actions of the FBI agents in obtaining and then executing what were essentially general warrants, cannot credibly be attributed to some reasonable oversight

or accident made under time pressure or otherwise driven by exigency.

To the extent that the Government tried to establish at the Hearing that the Apartment Search, at least, proceeded under time constraints presented by Michaela Wey's frustrations over the Search team's presence in her residence, the Court was unpersuaded. First, Agent McGuire testified that the FBI addressed Michaela Wey's concerns about the imminent return of her children with the "fairly simple solution" of completing its search of the children's rooms and play area first, specifically so that the remainder of the Search could be completed out of the children's presence. Hearing Tr. 255:19–256:4. More fundamentally, given the significant intrusion that inheres in any law enforcement search of the home in particular, it simply cannot be that a resident's impatience with FBI agents in her apartment, in and of itself, affords the Government cover to claim that any constitutional deficiencies reflected in its search were the product of rushed execution.

ii. Komar's Presence During the Searches

Second, while there can be no doubt that Agent Komar led both Search teams and was physically present on the scene for at least substantial portions of both Searches, the Government presented vanishingly little evidence that Komar's involvement *actually impacted* the overwhelming majority of seizure decisions made by FBI personnel executing the Warrants (which, as discussed further below, often resulted in the seizure of materials well beyond the scope of the Warrant applications). As noted above, Komar personally searched narrowly limited areas of the NYGG offices (the outer reception area) and the Wey Apartment (a guest room and portions of the children's rooms), and he seized only a few items relative to the overall Search take. *See supra* Sections I.D.2.–3. Although Komar testified that he generally recalled answering questions from team members regarding seizure decisions—testimony that the Court found, by and large, too vague and canned to be particularly persuasive—he could cite essentially no examples of instructions *not* to seize any materials based on non-responsiveness to the Warrants or the Warrant applications. And beyond that, the Government introduced zero evidence that Komar imposed any field constraints on the discretion of the agents who seized the overwhelming majority of the materials recovered from both locations. There was no suggestion, as noted above, that Komar directly supervised or double-checked any seizure decisions. Indeed, ASUA Massey testified that, to his understanding, seizure decisions were generally left to individual agents' "discretion," Hearing Tr. 67:18–68:20, and Agent McGuire (the only agent who seized a substantial ***401** portion of materials during either Search to appear as a Government witness at the Hearing) testified that he did not recall consulting any of his colleagues before making seizure decisions and generally made such calls based on his own understanding of the NYGG Warrant, *id.* 243:17–247:23, 298:13–299:1.

Based on the evidence before it, the Court simply cannot conclude that Agent Komar, while undisputedly onsite during both Searches, in fact meaningfully discharged any "respons[ibility] for ensuring that the items seized were within the scope of the approved search." *Rosa,* 626 F.3d at 59. Especially in light of *Groh's* rejection of the proposition that an agent may make up for a warrant's lack of particularity even by actually making certain that the search itself "did not exceed the limits intended by the Magistrate," 540 U.S. at 558–59, 124 S.Ct. 1284, the Court certainly does not read *Rosa* to suggest that an affiant's mere presence during a search may serve as a talismanic cure-all that automatically brings the execution of a grossly unparticularized warrant within the good faith exception. Accordingly, the second *Rosa* factor—Komar's personal involvement in the Searches themselves—has, at best, limited application here.

iii. Non–Reliance on the Defective Warrants

Third, and closely related, the Hearing failed to provide, and the record is otherwise devoid of, any credible evidence tending to show that the searching agents, in practice, cabined their own seizure discretion by "the contemplated limits of the search[es]," asset forth in the Komar and Garwood Affidavits, as opposed to by the four comers of the unparticularized Warrants themselves. *Rosa,* 626 F.3d at 64–66 (emphasizing, with approval, that the searching officers relied on "their knowledge of the investigation and the contemplated limits of the town justice's authorization," rather than "actually rel[ying] on the defective warrant"). As discussed, nothing in the record suggests that any of the more than twenty agents who participated in at least one of the Searches, other than Agents Komar and Garwood themselves, actually reviewed the Komar Affidavit or Garwood Affidavit prior to the Searches. And, critically, nothing suggests that the search team was ever otherwise informed of many of the

critical limiting details set forth in those Affidavits, such as which particular Issuers and Nominees were thought to be implicated in Wey's suspected scheme and the nature of their suspected involvement.

The Government maintains that the Operations Order and the pre-operations briefing led by AUSA Massey and Agent Komar provided the executing agents with sufficient information about the ongoing investigation "to be absolutely sure that the search team understood the scope" of, at least, "the NYGG Warrant." Gov't Supp. Opp. at 14. Even bracketing that it is the searching agents' grasp of the scope of the Warrant *applications*—rather than the scope of the Warrants themselves (which was essentially limitless)—that is the relevant consideration here, the Government's contention suffers from at least two critical flaws.

First, the Government provided no credible evidence suggesting that anything beyond high-level generalities was actually conveyed to the executing officers through the Operations Order or briefing. The Operations Order, as discussed, contained only two short paragraphs setting forth any substantive information at all about the investigation or the objectives of the NYGG Search, and that information amounted to, at best, a 30,000–foot summary—especially when contrasted with the detail set forth in the (unread, it appears) ***402** Komar Affidavit. The Order failed, for example, to identify any of the Issuers implicated in the suspected investigation, to in any way explain the relevance of the individuals and entities listed in Exhibit B, or to otherwise meaningfully link the items to be seized to the suspected crimes. *See* Gov't Ex. 1. For its part, the substantive portion of the pre-operation briefing consisted, according to Agent McGuire (the only beneficiary of the briefing called at the Hearing) of a "big-picture overview" of the investigation and the suspected criminal conduct, which he characterized as consistent with a "fairly typical securities fraud case." Hearing Tr. 239:17–21. Massey and Komar, who led the session, traded in similar generalities during the Hearing, largely failing to provide the Court with any insight as to the specific information conveyed to the agents in attendance. *See, e.g.,* Hearing Tr. 69:6–13 (Massey testifying that he did not "have a recollection of what I actually said" at the briefing); 124:12–15 (Komar testifying that Massey gave "examples of what we believed the scheme was essentially that we were investigating and communicat[ed] what types of documents ... we were going to be looking for").[13]

Second, even if the general gist of the Wey/NYGG investigation was arguably conveyed by the Operations Order and the case "overview" provided at the briefing, nothing suggests that any such instruction guided the agents' seizure decisions more so than did the Warrants' own sweeping terms. If anything, the Hearing testimony was generally to the contrary. AUSA Massey testified that the searching agents were tasked with exercising their "discretion" in "follow[ing] *what was in the warrant*"—not with executing some more limited vision of that document based on the Affidavits, the Operations Order, or the briefing. Hearing Tr. 68:12–20 (emphasis added). Agent McGuire—it bears repeating, the only search team member other than Komar to appear at the Hearing—testified that he made seizure decisions simply by referencing Exhibit B to the Warrants (the list of relevant individuals and entities that included NYGG and the Weys) and asking whether documents were "responsive to the search warrant" itself. Hearing Tr. 243:17–247:23. When later searching the electronically stored evidence, McGuire further testified, he made decisions about what to electronically "seize"—i.e., to tag as pertinent—based on whether they "covered by the warrant or not." *Id.* 292:9–21. Even Agent Komar himself, who conducted a limited initial review of a portion of the electronically stored evidence, asserted in a sworn declaration in support of the Government's original opposition to Wey's suppression motion that his review sought materials "falling within the parameters of the NYGG Warrant and the [Apartment Warrant]—that is, electronic documents and records of the kinds described in Exhibit ***403** A to the NYGG Warrant and the [Apartment Warrant] which concerned any of the entities or individuals in Exhibit B to those warrants." Komar Dec. ¶ 21.[14]

Consistent with that testimony, Government witnesses at the Hearing explicitly justified arguable examples of overseizure as falling "within the scope of the warrant." *See, e.g., id.* 56:20–57:7. For example and as noted above, AUSA Massey opined that medical prescription information sheets were subject to seizure under the relevant Warrant because they were related to the Weys' "personal expenses." *Id.* Massey similarly found "spreadsheets characterizing family medical issues" to be "within the scope of the warrant." *See* Def. Ex. 4 (e-mail memorandum from Massey). These candid concessions critically undermine, in the Court's view, the Government's post-hoc legal contention that the officers' discretion was meaningfully bounded by independent knowledge of the investigation.

The constitutional problem follows directly. The Warrants simply could not provide the requisite guidance to the searching officers because, as discussed at length above, they by their plain terms authorized the seizure of any record related to NYGG and/or the Weys. Critically, moreover, the record evidence reflects that is precisely how the Warrants were interpreted in practice by the Government agents responsible for their preparation and execution. As noted, AUSA Massey could think of no records beyond the scope of Exhibit A to Warrants (which listed the sorts of materials subject to seizure) other than "evidence ... of child pornography," illegal drug paraphernalia (but only if it did not have a written reference to NYGG on it), and an "al-Qaeda manifesto." Hearing Tr. 40:10–15, 48:2–10, 50:10–20. On the flip side, he agreed that "all the records of [NYGG] ... were in play" and subject to seizure, 14:8–10, 50:10–11, and that any "note," "memoranda," or "videotape"—even if decades old—was seizable if related to an individual or entity listed on Exhibit B, *id.* 46:23–47:3. Agent McGuire, for his part, thought it "very clear" that the Warrants covered, for example, "any financial records pertaining to the [Weys]," as well as all "financial records related to [NYGG]" and all "e-mails with [NYGG]." *Id.* at 276:12–20, 293:3–18, 304:11–14. On this record, the Court cannot find, as did the *Rosa* Court, that the scope of the Searches and the executing officers' discretion in making seizure decisions was in any way practically constrained by the limitations contemplated by the more specific Komar and Garwood Affidavits. Like any other aspect of the good faith inquiry, it is the Government's burden to establish as much, and the evidence submitted was simply unpersuasive and insufficient.

iv. Overseizure

Finally, there is the matter of overseizure. The *Rosa* Court took care to emphasize that there was "no evidence that the team of officers searched for, or seized, any items that were unrelated to the crimes for which probable cause had been shown." 626 F.3d at 65. Notwithstanding the Government's zealous efforts to persuade the Court otherwise, the same simply cannot be said here.

The agents seized, between the two search locations, a variety of hard-copy materials purely personal in nature, or otherwise plainly outside the scope of the suspected securities and wire fraud ***404** scheme described in the Affidavits.[15] As discussed above, these included medical records, prescription documents, X-rays, health care directives, educational records and scholastic mementos, divorce records, resumes, family photographs, recreational schedules, and other things. *See supra* Sections I.D.2.–3. To be sure, and as the Government emphasizes, several such items do appear to have been seized as part of larger sets of materials that could have been impractical to sort onsite (for example, the trash bag referenced above, which took something of a star turn in the Government's Hearing presentation) and thus were removed wholesale for offsite inspection. Gov't Supp. Opp. at 17. Even crediting such asserted logistical necessity as an explanation for some of these seizures, however, the record reflects that it does not apply to many others. *See, e.g.,* Def. Supp. Br. Ex. A (identifying examples); *see also* Gov't Ex. 14 (Evidence Recovery Log from Apartment Search noting seizure of multiple sets of materials identified onsite as "personal" documents, such as "school" and "immigration" records and "estate planning" documents).

In addition, it appears that following seizure, the Government completed pertinence review of these hard-copy materials by late 2012. To date, however, essentially none of the originals have been returned to NYGG or the Weys, Hearing Tr. 335:4–11, despite the requests of counsel—a potential constitutional violation in and of itself. *See, e.g., United States v. Tamura,* 694 F.2d 591, 596–97 (9th Cir. 1982) ("We likewise doubt whether the Government's refusal to return the seized documents not described in the warrant was proper."); *see also Ganias,* 824 F.3d at 230 (Chin, J., dissenting) (in cases where offsite review was required because "potentially relevant documents [were] interspersed through a large number of boxes or file cabinets," generally "non-responsive documents were to be returned after the relevant items were identified").

Perhaps more troubling than either the initial seizure or the continuing retention, however, are the efforts of the Government and its Hearing witnesses to leverage the inappropriately expansive terms of the Warrants into strained explanations of why these materials were in fact *properly* seized. *See, e.g.,* Hearing Tr. 56:17–57:7, 58:24–59:5, 59:25–60:7, 167:10–18, 304:24–305:3; Opp. at 40. Indeed, in maintaining, as discussed above, that children's school records, medical prescriptions, divorce records, and decade-old clippings from the sports section of the college newspaper among other things fell within the scope of the Warrants because they purportedly bore vague connections to the Weys' personal histories and finances, the Government and its agents leave the Court to find that much—perhaps even most—of the overseizure was not the result of expediency, mistake, or even

simple negligence. To the contrary, it seems, this material was reviewed, and a conscious effort was made to deem patently unresponsive materials responsive to the Warrants. Its presence in the Search fruits thus suggests that the execution teams affirmatively wielded the nearly unfettered discretion afforded them by the Warrants' expansive terms to appropriate documents that were perhaps of interest to some broader investigation of the Weys' lives and finances but that bore little or no discernible connection to the securities fraud probable cause showing actually submitted to the Magistrate Judge. *See, e.g.,* Hearing Tr. 276:14–20 ***405** (Agent McGuire testifying that it was "very important" that the FBI gain a better of understanding through the Searches of the Wey family's "very complex" "financial arrangements"). Put another way, it appears to be, as much as anything else, a product of the intentional execution of what amounted to general warrants.

b. The Government's Continuing Search of the Electronically Stored Evidence

This case presents still another factor, outside of the *Rosa* quartet, for evaluation in determining the Government's level of culpability and, correspondingly, its susceptibility in this context to deterrence. And it is one worth emphasizing: belying any argument that it sought to limit execution of the Warrants according to the parameters of the applications, the Government evinced no hesitation to subject the electronic Search fruits to continuing and, at least to some extent, expanding searches as its investigation and charging theories developed over the months and years following the initial Searches and preceding Wey's indictment.

As discussed above, AUSA Massey and Agent McGuire candidly testified at the Hearing that they had no qualms, for example, about searching the electronically stored evidence —well over a year after the Searches and prior to any sorting for pertinence—for evidence of tax evasion, an "alternative" charging theory not discussed in the Affidavits, apparently not developed until McGuire took over as case agent well after the Searches, and never presented to a judge. Similarly, they considered it within their authority to search the unsorted electronic materials for documents pertaining to a number of individuals and entities not identified or discussed in the Warrants or the applications but whose potential relevance to the ongoing investigation became increasingly apparent sometime after the Searches concluded (Defendant Erbek, for example). *See supra* Section I.D.4.b.

The Government maintains that this approach to reviewing the electronic evidence was entirely appropriate so long as its novel search terms were designed to identify documents that would otherwise fall within the Warrants' (inappropriately expansive) terms. Indeed, when questioned about the continuing searches at oral argument, the Government appeared to take the somewhat surprising position that it would be well within the Government's rights to search retained electronic materials that it had *already deemed unresponsive* to the Warrants using "[a]ny word" the Court could think of as a search term. It would not matter, according to the Government, whether the search bore any connection whatsoever to the actual terms of the Warrants or even how much time had elapsed since the Warrants' issuance. *See, e.g.,* Oral Argument Tr. 12:9–17:11.

As was elicited at the Hearing, moreover, it would seem that such a position was no mere hypothetical. Crediting Agent Miller's version of the pertinent events as explained above, the Court finds that in mid to late 2015 (some three-plus years after the Searches and with a grand jury presentation in the works), the FBI arranged to have Agent Miller run searches across *all* recovered electronic evidence, including that portion earlier deemed unresponsive by Agent McGuire, for documents concerning topics (again, Erbek is an example) not addressed by the Affidavits or Warrants. It evidently saw no need to prepare Agent Miller for this exercise beyond a cursory overview of the case and a review of some "examples," choosing not to arrange briefing or training on the scope of the Affidavits or the Warrants. *See supra* Section I.D.4.b.

***406** Wey urges that this conduct is independently violative of the Fourth Amendment. It may be. Regardless, the Court finds that, if nothing else, it constitutes further evidence of the agents' culpability in making affirmative choices to treat the Warrants as though they were the functional equivalent of general warrants. Such conduct can and should be deterred.

First, the record does not support the factual premise that forms the core of the Government's argument as to the propriety of these later searches: that the only documents that could be deemed pertinent—and thus electronically "seized"—during this process were those that were independently subject to seizure based on the Warrant themselves. Agent McGuire, who, as discussed, conducted searches using an expanded list of search terms in mid–2013, testified that he generally did not even review all

documents returned by a term-based search before deeming them wholesale pertinent. Rather, after running such a search, he would review a sample of the returns, make a preliminary determination as to whether the search term appeared to yield at least some returns arguably within the Warrants' scope, and then proceed to "seize" the entire set with no further document-by-document review. Hearing Tr. 289:1–20; 292:9–294:3. With respect to certain extra-Warrant search terms (such as "Erbek"), McGuire further testified that their presence in a document could be enough, in and of itself, to merit a pertinence tag based on his evolving understanding that, for example, documents pertaining to Erbek tended to concern financial matters. *Id.* 351:1–352:1. As for Agent Miller's 2015 searches, the Government simply offered no evidence through any witness with direct knowledge of the process that only documents previously identified as pertinent were tagged by Agent Miler. *See id.* 339:9–341:7 (McGuire conceding that he did not participate in the actual searches and never viewed electronic records thereof); *id.* 374:2–375:23 (Miller testifying that McGuire provided her with, at the most, two or three documents as "examples" to help guide her searches and that she then tagged as pertinent possibly as many as fifty or more documents in the FBI databases).

Furthermore, the Government cites, and the Court is aware of, no authority suggesting that simply because it has retained all originally searchable electronic materials, the Government is permitted to return to the proverbial well months or years after the relevant Warrant has expired to make another sweep for relevant evidence, armed with newly refined search criteria and novel case theories.

Perhaps most plainly problematic on this score are Agent Miller's 2015 searches which, as noted, covered all documents in the FBI databases, including those materials *already sorted out as impertinent* two years earlier. Clearly, as the defense urged at oral argument, additional physical searches in 2013 or 2015 of hard-copy documents judged irrelevant and left behind during the NYGG Search or the Apartment Search would have been presumptively impermissible—new search terms or not—in the absence of a fresh warrant. *Cf. Ganias,* 824 F.3d at 212–213 (recognizing that, though perhaps "imperfect," the analogy between searches of physical files and electronic files "has some force, particularly as seen from the perspective of the affected computer user," and "ha[s] some relevance" to the Fourth Amendment inquiry"). Indeed, the proper analogy to help appreciate the nature of the agents' conduct here is not the Government seizing, for example, a hard-copy notebook deemed responsive to a warrant, retaining it, and later returning to that notebook for follow-up searches as its investigation developed. Instead, Agent Miller's searches are akin ***407** to the Government seizing some hard-copy notebooks while leaving others it deemed unresponsive behind, and then returning to the premises two years later to seize the left-behind notebooks based on investigative developments but without seeking a new warrant.

The stark contrast between the Government's conduct on this front and its conduct in *Ganias*—a recent Second Circuit decision focused on the retention and search of computer data—underscores this point. In *Ganias,* agents from the United States Army Criminal Investigation Division obtained, pursuant to a warrant, forensic mirrors of all data stored on several computer hard drives in an accountant's office as part of an investigation that targeted two of the accountant's clients—but not the accountant himself. The Government searched the data and identified and segregated relevant files within a few months, but then retained all of the recovered data (not just that deemed relevant) for several more years. Approximately three years after the execution of the original warrant, the Government independently developed probable cause to believe that the accountant was personally involved in a tax evasion scheme. Understanding that it could not unilaterally re-search the mirrored data in its possession that it had previously sorted out as non-responsive to the original warrant (such as the accountant's personal financial records and records of clients not targeted by the original investigation), the Government *applied for a new search warrant* and made clear in its application that it wished to run new searches over electronic materials that had been in its custody, and assumed irrelevant, for several years. After securing and executing a fresh warrant to search that data, the Government indicted the accountant. The Circuit, sitting *en banc*, upheld the later search under the good faith exception in large measure because the Government *had acted reasonably in applying for the second warrant and alerting the magistrate to the circumstances. See Ganias,* 824 F.3d at 200–07, 224–26.

For the Government to skirt that new-warrant obstacle here by—appearances would suggest—intentionally taking advantage of its sweeping electronic take to look for evidence in an essentially analogous manner is inconsistent, in the Court's view, with a claim to good faith in executing the Warrants.

The Second Circuit's recent discussion of electronic searches in *Ulbricht* is not to the contrary. There, the Defendant argued in pertinent part that a warrant authorizing the search of his laptop computer was insufficiently particularized because it did not "specify the search terms and protocols" to be used in reviewing the contents of the laptop "*ex ante*." 858 F.3d at 101–04. The Court of Appeals disagreed, reasoning that "it will often be impossible to identify in advance the words or phrases that will separate relevant files or documents before the search takes place, because officers cannot readily anticipate how a suspect will store information related to the charged crimes"—a concern that was viewed as particularly reasonable in the context of the investigation at issue, which targeted an individual suspected of running an online marketplace for illegal goods and services that "us[ed] sophisticated technology to mask its users' identities." *Id.* at 102. Here, Wey does not argue, and the Court does not conclude, that the Warrants were insufficiently particularized due to any failure of their electronic search protocols to incorporate search term lists *ex ante.* The Court fully recognizes, moreover—as the *Ulbricht* Court took care to emphasize—that privacy invasions are inevitable in searches of electronic data and that the Government may ***408** "come across personal documents ... unrelated to [the defendant's] crimes" in the course of executing such searches without running afoul of the Fourth Amendment. *Id.* at 103. But nothing in *Ulbricht,* or in any other authority of which the Court is aware, permits the Government to sit on eighteen terabytes of data for years after the expiration of the authorizing warrant and intentionally mine it with searches targeting individuals and charging theories absent from the warrant application but identified as relevant by post-search developments in the Government's investigation. It should also be noted that the warrant in question in *Ulbricht* provided robust limitations on what electronic documents could ultimately be seized, regardless of the search terms used to identify them. *See id.* at 99–104 (explaining that the warrant and the explicitly incorporated underlying affidavit, among other things, identified the relevant crimes and specifically "connect[ed] the information sought to the crimes charged"). The utter lack of similar limitations in the Warrants at issue here—especially when combined with the agents' unrestrained interpretation of their seizure authority under those Warrants—makes the Government's use of a continually expanding search term list to identify documents of interest all the more troubling as a practical matter.

* * *

As the Court of Appeals has observed, "[g]ood faith is not a magic lamp for police officers to rub whenever they find themselves in trouble." *United States v. Reilly,* 76 F.3d 1271, 1280 (2d Cir. 1996).

Government agents leading a long-running, well-resourced investigation took weeks or months to draft proposed Warrants that were plainly lacking the basic features called for by the Fourth Amendment's particularity requirement and whose scope, partially as a result, grossly exceeded the probable cause showing ultimately made to the Magistrate Judge. Upon issuance of those Warrants, the agents deployed the trappings of good faith—an Operations Order, a briefing—while dispensing with more robust safeguards such as a requirement that the search personnel read the Affidavit, and then proceeded to conduct sweeping physical and electronic searches lacking in any discernible parameter beyond the inappropriately broad terms of the Warrants themselves. Interpreting and executing their authority expansively—in keeping, the evidence suggests, with the intention of the drafters—the agents treated the Warrants both during and after the physical Searches as, for all intents and purposes, general warrants.

The Court does not conclude that the agents acted with malice. But it does find that their conduct cannot be credibly explained by exigent circumstance, by simple mistake, or by mere negligence. The agents—who are charged with reasonable knowledge of what the law prohibits—appear to have disregarded well-established constitutional principles that provide a bulwark against the execution of general warrants. That reflects, at the least, gross negligence or recklessness as to the potential for violation of the Fourth Amendment. It cannot be that a facade of particularity and reasonableness built on superficial checkmarks in the *Rosa* boxes brings that conduct within the good faith exception. Echoing Judge Oetken in *Zemlyansky,* "[t]his conduct is deferrable, and the Constitution requires its deterrence." 945 F.Supp.2d at 476.

For these reasons, the Court cannot, on the record before it, find that the Government has carried its burden on the good faith question. The Court is mindful that "the Supreme Court [has] strongly signaled ***409** that most searches conducted pursuant to a warrant would likely fall within [the] protection" of the exception. *Clark,* 638 F.3d at 100 (citing

Leon, 468 U.S. at 921–922, 104 S.Ct. 3405). Nevertheless, it remains "clear that in some circumstances the officer will have no reasonable grounds for believing that the warrant was properly issued." *Leon*, 468 U.S. at 922–93, 104 S.Ct. 3405 (footnote omitted); *see also Ganias,* 824 F.3d at 221 (reaffirming that reliance on a later invalidated warrant "must be *objectively reasonable*" to trigger the good faith exception) (emphasis in original). Finding such circumstances here and finding the conduct of the Government agents in obtaining and executing the Warrants to be both culpable and deferrable, the Court concludes that the good faith exception has no application to the Searches at issue. Accordingly, suppression is warranted.

D. Remedy

Having determined that the Warrants do not comport with the Fourth Amendment and that the Searches cannot be salvaged by the good faith exception, what remains is the question of the appropriate remedy.

As a preliminary matter, the Court recognizes the Second Circuit's directive that, to the extent possible, constitutionally infirm warrants should generally be assessed for the prospect of severability, and infirm searches for the possibility that any of the challenged evidence was in plain view when seized. *See, e.g., Galpin,* 720 F.3d at 448. Here, the Government has largely waived any substantive argument as to severability, even despite an express invitation to do so at oral argument. *See* Oral Argument Tr. at 77:20–78:10. In any event, the Court easily concludes that the Warrants are not severable. The primary deficiencies described above—the lack of reference to any crime under investigation, the absence of linkage between seizable items and suspected criminal conduct, the "limitation" only by relation to the Weys or to NYGG—apply to substantially every provision of Exhibit A to both the Warrants, and, accordingly, they "taint each of the ... [W]arrants *in toto*." *Hickey,* 16 F.Supp.2d at 244. As *Galpin* itself instructs, severance is usually "not an available remedy" if "no part of the warrant is sufficiently particularized ... or where the sufficiently particularized portions make up only an insignificant or tangential part of the warrant." 720 F.3d at 448.

As for the plain view doctrine, it is the Government's burden to demonstrate, if it so chooses, that specific seized items fall within that exception to the Fourth Amendment's requirements, and the Government here has not developed any evidentiary record that would allow the Court to reach such a conclusion. Indeed, as discussed above, the Government declined to call as Hearing witnesses the agents who actually seized the overwhelming majority of the items taken during both Searches. Accordingly, the Court cannot apply the exception to salvage any particular portion of the evidence seized during the Searches. *See, e.g., United States v. Kiyuyung,* 171 F.3d 78, 83–85 (2d Cir. 1999) (rejecting plain-view argument because Government failed to develop sufficient evidentiary record).

Unable, then, to further tailor the remedy according to the severability or plain view doctrines, the Court concludes that suppression of all evidence seized during the courses of both Searches is the only appropriate recourse under the circumstances. Of some note, the Government—again given the express opportunity—declined to submit any concrete alternative remedy for the Court's consideration. *See* Oral Argument Tr. 77:4–78:10 (submitting ***410** only, in sum and substance, that "wholesale suppression ... would be too severe" and that the Court should limit any suppression "to where the Court believes the government sort of went too far or acted unreasonably"). Even in the absence of meaningful input from the Government, however, the Court recognizes the gravity of its decision and does not reach it lightly. "[W]holesale suppression," of the sort urged by Wey, is generally considered an extraordinary remedy, appropriate only when (1) government agents "effect a widespread seizure of items that were not within the scope of the warrant," and (2) "do not act in good faith." *Shi Yan Liu,* 239 F.3d at 140 (internal quotation marks and citations omitted). "[T]o satisfy the first prong ... the search conducted by government agents must *actually resemble* a general search." *Id.* at 141. "The rationale for blanket suppression is that a search that greatly exceeds the bounds of a warrant and is not conducted in good faith is essentially indistinguishable from a general search." *Id.* at 141; *see also Cardwell,* 680 F.2d at 78 ("If no portion of the warrant is sufficiently particularized to pass constitutional muster, then total suppression is required. Otherwise the abuses of a general search would not be prevented.") (internal citation omitted); *United States v. Rettig,* 589 F.2d 418, 424 (9th Cir. 1978) (ordering blanket suppression where, "[a]s interpreted and executed by the agents, this warrant became an instrument for conducting a general search" and, "[u]nder the circumstances, it [was] not possible for the court to identify after the fact the discrete items of evidence which would have been discovered had the agents kept their search within the bounds permitted by the warrant"); *cf. United States v. Medlin,* 842 F.2d 1194, 1199 (10th Cir. 1988) ("When law enforcement officers grossly exceed the scope of a search warrant in seizing property, the particularity requirement is

undermined and a valid warrant is transformed into a general warrant thereby requiring suppression of all evidence seized under that warrant.").

For all of the reasons discussed at length above, however, that scenario—unusual though it may be—is the one facing the Court. The Government took weeks or months to apply for Warrants facially lacking in particularity and so sweepingly broad in the scope of their proposed authorization as to exceed the probable cause showing submitted to the Magistrate Judge. As issued, those Warrants, by their terms, authorized essentially limitless search and seizure —targeting all documents in both the NYGG offices and the Wey Apartment, regardless of their potential connection to any criminal conduct and bounded only by the illusory "limitation" that they relate to NYGG or the Weys. The searching agents, interpreting that authority expansively and unconstrained (the Court has found) by the superficial extra-Warrant safeguards the Government trumpets as evidence of good faith, proceeded to execute the Warrants as though they were the functional equivalents of general warrants, in both their indiscriminate physical searches and seizures and, later, their expanded mining of the retained electronic take for evidence related to new persons and new crimes. This conduct reflects, at least, grossly negligent or reckless disregard of the strictures of the Fourth Amendment, and that is sufficient to infer a lack of good faith. In the Court's view, these are precisely the sort of circumstances, rare or not, that call for blanket suppression.

III. Conclusion

For the reasons set forth above, Wey's motion to suppress evidence is GRANTED in its entirety. Because the Court reaches this conclusion based on the Warrants' ***411** lack of particularity and overbreadth, it does not reach Wey's alternative arguments that the Affidavits submitted in support of the Government's warrant applications were misleading or that the Government's long-standing retention of the evidence recovered during the Searches constitutes a Fourth Amendment violation in and of itself.

In light of the suppression remedy that it hereby orders, the Court also views it as unnecessary to address Wey's application to preclude the Government from further reviewing any potentially privileged documents seized during the Searches and to compel the Government to disclose information about the review process. If the parties think otherwise, they shall set forth their respective positions in letter-briefs, not to exceed three pages in length, within fourteen days of this Order.

Wey's separate motion to seal certain evidentiary exhibits submitted in support of his post-Hearing supplemental brief, *see* Def. Supp. Br. Exs. A–C, is GRANTED. The relevant materials reflect sensitive medical, financial, educational, and other personal information pertaining to non-parties, and the Court finds that the privacy interests of those non-parties outweigh any public interest in disclosure, whether derived from the First Amendment or the common-law right of access, and that the sealing application is narrowly tailored to serve those interests. *See Lugosch v. Pyramid Co. of Onondaga*, 435 F.3d 110, 124 (2d Cir. 2006).

Finally, it is ORDERED that, within fourteen days of this Order, the parties shall meet and confer and jointly submit a letter proposing a schedule to govern all remaining pretrial proceedings, including the submission of motions *in limine* and other pretrial materials.

This resolves Dkt. No. 44.

SO ORDERED.

All Citations

256 F.Supp.3d 355

Footnotes

1 The Court notes that Nasdaq's decision was subsequently set aside on review by the Securities Exchange Commission ("SEC"). *See In re Application of CleanTech Innovations, Inc.,* Exchange Act Release No. 69968, 2013 WL 3477086 (Jul. 11, 2013).

2 Following the Hearing and at the Court's direction, the Government submitted for the Court's reference a binder containing all documentary and electronic exhibits entered into evidence by the parties. The index to that binder is being filed concurrently with this Opinion and Order as Court Exhibit 1.

3 In roughly the same timeframe and further reflecting the shifting focuses of the Government's investigation and its evolving theories of its case, AUSA Massey became aware through conversations with FBI analysts that some of the electronic data recovered during the Searches—including data that the Government had already shared with the SEC to aid its parallel of investigation of Wey—included documents of "a purely personal nature," such as "spreadsheets reflecting family medical issues." Def. Ex. 4 (May 3, 2013 e-mail memorandum to file by Massey); Hearing Tr. 77:8–78:4. In a May 2013 memorandum to file, Massey rationalized the seizure of such documents as "within the scope the warrant because Wey's tax returns are relevant documents because we believe he committed tax fraud, and he claimed large medical deductions most years." Def. Ex. 4; Hearing Tr. 79:5–20. Once again, neither tax fraud nor any other scheme involving medical deductions was presented to Magistrate Judge Dolinger or communicated to the Search teams as a current subject of Government interest at the time of the Searches. *See, e.g.,* Hearing Tr. 78:17–79:16, 80:7–14.

4 As a threshold matter, a defendant "seeking to suppress the fruits of a search by reason of a violation of the Fourth Amendment" generally "must show that he had a 'legitimate expectation of privacy' in the place searched." *United States v. Hamilton,* 538 F.3d 162, 167 (2d Cir. 2008) (quoting *Rakas v. Illinois,* 439 U.S. 128, 143, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978)). "Where the premises searched is a business, defendants seeking suppression must establish both that they are associated with the business and that they have a legitimate expectation of privacy in the part of the business that was searched." *United States v. Kazarian*, 10–cr–895, 2012 WL 1810214, *18 (S.D.N.Y. May 18, 2012) *(citing O'Connor v. Ortega*, 480 U.S. 709, 718, 107 S.Ct. 1492, 94 L.Ed.2d 714 (1987)). Here, the parties do not appear to dispute that Wey has standing to challenge the Search of his residence or the Search of the offices of NYGG, a private firm of which Wey was founder and chief executive officer.

5 As the Government correctly observes, the Second Circuit's *Galpin* decision, cited above, post-dates the Searches at issue. *See* Government's Memorandum of Law in Opposition to Defendant Benjamin Wey's Motions to Suppress Evidence, Prevent a Privilege Review, Dismiss the Indictment, Take His Co–Defendant's Deposition Abroad, and Strike References to Aliases, Dkt. No. 53 ("Opp."), at 30. The Court does not view that fact as material to its analysis of the Warrants. It may be true that prior to *Galpin,* the Circuit had not necessarily articulated one "settled formula for determining whether a warrant lacks particularity." *Zemlyansky,* 945 F.Supp.2d at 453. Still, the requirements outlined in *Galpin* are hardly novel, and each had been clearly idenfitied on an individualized basis well prior to the advent of the comprehensive *Galpin* framework—and, more importantly, well prior to the Searches. Indeed, the *Galpin* Court itself cited at least one earlier Circuit decision in support of each requirement it enumerated and in no way purported to break any ground in marshalling that law. 720 F.3d at 445–446. Still further, well before *Galpin,* courts in this District surveying the particularity case law consistently recognized at least two discrete "factors" that "tend to define a warrant's insufficient particularity." *See, e.g., United States v. Vilar*, 05–cr–621, 2007 WL 1075041, at *21–22 (S.D.N.Y. Apr. 4, 2007) (collecting cases). Those factors substantially track the two item-related requirements explicitly set forth in *Galpin*: (i) the failure to "tell[ ] the searching officers for what crime the search is being undertaken" and (ii) the inclusion of "general catch-all paragraph[s] or provision[s], often ... authorizing the seizure of 'any and all records' of a particular type." *Vilar,* 2007 WL 1075041, at *21–22 (internal quotation marks and citations omitted) (collecting cases); *see also Zemlyansky,* 945 F.Supp.2d at 453–54 (same). Accordingly, the Court is satisfied that the intervention of the *Galpin* decision is of no particular moment on this point one way or the other.

6 Nor, on a similar note, does the Warrants' single passing reference to seizing "property purchased with the proceeds of fraud," NYGG Warrant Ex. A. ¶ 10, substitute for the requisite identification of the crime under investigation. *See, e.g., United States v. Vilar,* 2007 WL 1075041, at *22 ("oblique reference" in warrant rider to " 'participants in fraud schemes' " could not cure warrant's failure to "indicate what specific acts of wrongdoing are being investigated"); *see also Galpin,* 720 F.3d at 445 n.5 (because the "purpose" of the requirement that the crime be identified is "to minimize the discretion of the executing officer, other Circuits have held that even warrants that identify catchall statutory provisions, like the mail fraud or conspiracy statutes, may fail to comply with this aspect of the particularization requirement") (collecting cases).

7 Other courts in this Circuit have concluded that similarly expansive categories of documents rendered warrants constitutionally deficient. *See, e.g., United States v. Bianco,* 998 F.2d 1112, 1115–1116 (2d Cir. 1993) (warrant for home authorizing seizure of "[n]otes, ledgers, envelopes, papers, and records containing initials, names, addresses, dollar amounts, codes, figures, and the like" was insufficiently particularized especially when such items were not "tied to particular crimes"), *abrogated on other grounds by Groh,* 540 U.S. at 557, 124 S.Ct. 1284; *Buck,* 813 F.2d at 591 (warrant consisting entirely of "general boilerplate terms, without either explicit or implicit limitation on the scope of the search" was

insufficiently particularized); *Zemlyansky,* 945 F.Supp.2d at 457–59 (no particularity where warrant authorized seizure of, among other things, "checks, cash, and other financial instruments," "bank account information," "calendars and patient appointment records," and "records related to patient care"); *Hernandez,* 2010 WL 26544, *10 (warrant to search business offices likely lacked particularity because it "could have encompassed most all of the business records on the premises"); *Vilar,* 2007 WL 1075041, at *22–23 (warrant provision authorizing seizure of all "corporate records" concerning the occupant of the premises and its affiliates reflected "patent lack of particularity," notwithstanding inclusion of illustrative list of items); *United States v. Hickey,* 16 F.Supp.2d 223, 237–241 (E.D.N.Y. 1998) (warrant authorizing seizure of "all business records" of four companies, "including but not limited to" approximately fifty individually listed generic items, was deficient); *United States v. Gigante,* 979 F.Supp. 959, 966 (S.D.N.Y. 1997) (warrant provision permitting seizure of "financial, banking, safe deposit, investment, asset, tax, bookkeeping, and accounting records," along with "underlying, supporting, and related documentation," of "or referring or relating to" several named individuals lacked particularity).

8 USA Massy conceded at the Hearing that he had read portions of the Government's briefing on Wey's suppression motion and was aware that it was pressing an argument based on the all-records exception. Hearing Tr. 32:22–33:4.

9 "[W]hen multiple officers are involved in an illegal search, 'it is necessary to consider the objective reasonableness, not only of the officers who eventually executed a warrant, but also of the officers who originally obtained it or who provided information material to the probable-cause determination.' " *Zemlyansky,* 945 F.Supp.2d at 476 (internal brackets omitted) (quoting *Leon,* 468 U.S. at 923 n.24, 104 S.Ct. 3405).

10 Invoking this reasoning, Wey advances the threshold argument that the Warrants are so facially deficient that the good faith exception is, essentially, unavailable to the Government. Supp. Br. at 3–5. Because, as discussed further below, the Court concludes that the good faith exception has no application to this case under even the arguably more generous interpretation of the doctrine signaled by more recent Supreme Court and Second Circuit decisions, it need not, and does not, address that argument.

11 *Zemlyansky,* 945 F.Supp.2d at 468.

12 Because the Court reaches this conclusion with respect to the Warrants' lack of particularity, it does not separately consider—to the extent that it would implicate an independent analysis—whether an objectively reasonable officer could have relied on the Warrants notwithstanding their overbreadth.

13 All of this assumes that even a thorough and detailed briefing on the contemplated limits of the Magistrate Judge's authorization could potentially bring the otherwise constitutionally infirm search within the good faith exception—a proposition about which at least one court in this District has expressed considerable doubt. *See Zemlyansky,* 945 F.Supp.2d at 473–74 (recognizing both that a "briefing session generates substantial room for slippage between the magistrate's authorization and the searching officers' understanding of their authority" and that the "historic notice function served by a lawful warrant," as emphasized in *Groh,* would "fall by the wayside if officers could claim good faith each time" they had simply "been briefed about the affidavit" before the search); *see also Vilar,* 2007 WL 1075041, at *8, 22 n.13 (notwithstanding pre-search briefing, there was "no certainty that all members of the search team were aware of the limits, if any, to be read into the Warrant from the supporting documents").

14 At the Hearing (which, of course, the Court explicitly convened to address the good faith question), Komar changed his tune, testifying that he relied primarily on his "knowledge of the case" rather than on "search materials"—an assertion the Court found less than persuasive. Hearing Tr. 153:13.

15 That is to say nothing of the more than 100,000 electronic documents ultimately seized by the Government, examples of which—to the Court's understanding—have largely not been put before it.