4. In Thomas v. City of New York, 336 F.R.D. 1 (E.D.N.Y. 2020), Magistrate Judge Sanket J. Bulsara granted Plaintiff's motion to compel production of ESI, including emails, text messages, and GroupMe chats, where Defendants failed to overcome Plaintiff's showing that the requested discovery was not relevant and proportional and did not show that the discovery was not reasonably accessible because of undue burden or cost.

Plaintiff in this civil rights action sought ESI from Defendants, including emails, text messages, and GroupMe chats. Id. at *1. Defendants agreed to collect and produce certain categories of the requested documents from a subset of Defendants but opposed any additional collections or productions. Id. at *1-*2. In response, Plaintiff filed a motion to compel production of the remaining documents it had requested.

Magistrate Judge Bulsara began by setting forth the general standard under Rule 26 of the Federal Rules of Civil Procedure: "Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case." If the requests are relevant and proportional, the objecting party has the burden of showing that the requests should nonetheless be denied. As to ESI specifically, to avoid production, "the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost."

First, as to relevance and proportionality, Defendants argued that having collected a subset of what Plaintiff requested from some defendants, any additional collection would not yield any unique or nonduplicative information. Yet Magistrate Judge Bulsara found that Defendants failed to offer any evidence to substantiate their position, "such as email exhibits showing that all parties were copied on the relevant emails," or a plausible explanation, "such as a factual proffer that, given their roles as supervisors, these defendants always emailed with each other about all employees." "The mere fact that many documents have already been produced is not sufficient to establish that there are no other relevant materials to be found." Id. (internal quotations marks omitted).

Furthermore, for Defendants to prevail on limiting discovery because of duplication, they must show that the information at issue is "unreasonably cumulative or duplicative." Id. (internal quotation marks omitted). But the fact that there may have been some overlap and duplication "is insufficient to preclude the discovery sought." Additionally, as Magistrate Judge Bulsara observed, "even if duplicative, obtaining the information about custodian of a text message or email yields pertinent information." Id. at *3. "[E]ven if an email was produced from one witness's custodial inbox, producing the same email from another witness's inbox establishes that the second witness received the email (and helps counter any suggestion that he or she lacked knowledge of or did not receive the email in question)."

Second, Magistrate Judge found that "Defendants' papers are devoid of any specific analysis of the burden of the ESI production being sought by Plaintiff." Accordingly, Magistrate Judge Bulsara held, "the Court cannot conclude that the efforts in reviewing the ESI of the additional custodians would be so burdensome so as to be 'inaccessible.' "

Magistrate Judge Bulsara continued that "[i]t appears — though the parties' papers are unclear on this point — that Defendants have agreed to obtain a subset of ESI from particular defendants and cobbled together the information." However, "[t]his kind of splicing — collecting emails from one defendant, text messages from another — with the hope that the amalgam of information is the universe of relevant discovery is an inappropriate collection and production methodology" because "[i]t assumes, [falsely,] that one person's documents are complete and nothing has been deleted or expunged, that reviewing duplicate information is unduly burdensome or disproportionate, and that custodian information is irrelevant." The magistrate judge also rejected Defendants' argument that they were best situated to determine which custodians to search because this approach "is in tension with Rule 26 — which requires production of ESI unless 'the party resisting discovery [has] shown that the information in question is not reasonably accessible.' " Id. at *4. (emphasis in original). Defendants also argued that "in other districts Plaintiff[ ] would not be permitted to discovery from other custodians — i.e., there is an automatic limit." But Magistrate Judge Bulsara clarified that the relevant issue was "whether the discovery is relevant and proportional, not whether ... Plaintiff's request exceeds a bright-line cap."

Magistrate Judge Bulsara rejected Defendants' proposal to collect text messages from one of the three requested custodians, "who was part of all of the text messages of all three." Id. *4-5. "Defendants['] attempt to avoid text message collection from these individuals because they have said there are no other text messages is unpersuasive, particularly when there has been no showing that there is a disproportionate burden from the additional collection and production." Id. at *5. With respect to GroupMe chats, Magistrate Judge Bulsara rejected Defendants' position that "custodial interviews reveal there was nothing relevant to this lawsuit discussed on the chat" because it represented "a form of self-collection which is strongly disfavored." Magistrate Judge Bulsara similarly rejected Defendants' argument that by deleting his copy of the requested chats, Plaintiff admitted their nonrelevance: "Defendants have a preservation and production obligation irrespective of whether Plaintiff complied with any obligation he had." Accordingly, Magistrate Judge Bulsara granted Plaintiff's motion to compel and ordered Defendants to collect and produce the remaining requested categories of documents from all Defendants.

5. In In re Search of Info. Stored at Premises Controlled by Google, 2020 U.S. Dist. LEXIS 152712 (N.D. Ill. Aug. 24, 2020), a case in which "geofence" warrants faced their first round of judicial scrutiny, Magistrate Judge Gabriel Fuentes denied the government's proposed search warrant application because it failed to satisfy the Fourth Amendment's probable cause and particularity requirements.

In this case, the government sought a "geofence" search warrant to obtain data from Google in connection with an investigation into a suspected theft of prescription medications. Id. at *1. Generally, geofence search warrants allow law enforcement to search a database to find all active mobile devices within a defined geofence area. While conducting its investigation, the government developed evidence, in part from surveillance footage, suggesting that an unknown individual entered two physical locations to receive and ship stolen medication at specific times. Id. at *1-2. In hopes of identifying the individual, the government submitted an application for a geofence search warrant seeking historical information from Google, which would identify devices that were at those locations around the times the suspected thefts took place. Id. at *1.

Google collects location data from sources including GPS information, cell-site information, Wi-Fi access points, and Bluetooth beacons within range of a given mobile device. Id. at *5. Devices with Android as well as Apple operating systems communicate with Google when a user enables "location services" (for Android devices) or "location sharing" services (for non-Android devices).

This information can show that a certain device was located at a particular place at a particular point in time, and, as the government suggested, a device that does not transmit this type of location information to Google "would be a relatively rare case." Id. at *6-7.

The government's application sought to set up three geofences. Id. at *2. Two would be at the same location but would cover different timeframes. The third would be at a second location. The timeframe for each proposed geofence would be 45 minutes. For each of the proposed geofences, the government requested that Google be compelled to disclose a list of unique device identifiers for devices known by Google to have traversed the respective geofence. The government hoped to use this information to help identify the unknown suspect — the theory being that at least one of the devices identified by Google to have traversed a geofence would likely belong to the individual seen on surveillance footage.

The government submitted two prior applications, both of which were denied. The first application was denied on July 8, 2020, by Magistrate Judge M. David Weisman. Id. at *2-3. The second application "narrowed the geographical scope of the three proposed geofences, drawing them more tightly around the two physical locations where the [unknown suspect] was seen entering to receive or ship the stolen medication, and attempting to reduce the number of devices (and persons) identified in the search." Id. at *3. Magistrate Judge Fuentes denied the government's second application on the grounds that it failed to meet the Fourth Amendment's probable cause and particularity requirements.

In its third application, the government attempted to narrow the warrant by altering the proposed search protocol to eliminate the third of the three stages set forth in the prior warrant applications. The three stages were "(1) Google's collection of information it possesses about devices it believes traversed the geofences; (2) Google's production of an 'anonymized' list of the unique device IDs for those devices as well as related information including their location coordinates and time stamps; and (3) Google's production of the subscriber information identifying the account holders or users of the devices on the anonymized list, with the government exercising its discretion as to the device IDs for which Google would obtain identifying subscriber information and provide it to the government." The government argued that eliminating the third stage would cure the warrant application of any of the previously identified constitutional deficiencies. In particular, the government contended that the revised application survived constitutional scrutiny because it "d[id] not seek any individual identifying information and cannot be used to identify a device's user without further information from Google." Id. (internal quotation marks omitted). The government also amended the description of the information to be seized by limiting the anonymized information to that which "identifies individuals who committed or witnessed the offense," which it argued would bring the warrant into compliance with the particularity requirement by limiting the government's discretion "to select device information from among the anonymized lists." Id. at *5 (internal quotation marks omitted). Additionally, the government added a representation that it would retain the power to obtain by subpoena the identifying subscriber information for any of the device IDs on the anonymized list obtained under the proposed warrant but that the government would do so only after reviewing the anonymized information.

Magistrate Judge Fuentes began his analysis by considering whether the third application proposed a search for purposes of the Fourth Amendment. Id. at *7. As he explained, "[a] government intrusion into a person's private sphere qualifies as a search, triggering the Fourth Amendment requirement that the intrusion be authorized by a warrant supported by probable cause, when that person seeks to preserve something as private, and his expectation of privacy is one that society is prepared to recognize as reasonable." Id. (internal quotation marks omitted). Although the magistrate judge recognized that recent Supreme Court precedent "raises questions about the degree to which ... the proposed geofences constitute a search," he ultimately chose not to reach the question in this case. Instead, he concluded that because the government treated the proposed receipt of information as a search, arguing that it satisfied the Fourth Amendment, the government thereby forfeited any argument that the Fourth Amendment did not apply. Id. at *12-13.

Magistrate Judge Fuentes next considered whether the application satisfied the Fourth Amendment's probable cause and particularity requirements. Id. at *21. On probable cause, Magistrate Judge Fuentes concluded that despite the government's tweaks, the third application "suffer[ed] from the same probable cause problem as did the earlier two applications." Id. at *41. Specifically, according to Magistrate Judge Fuentes, "[b]ecause the proposed warrant here s[ought] information on persons based on nothing other than their close proximity to the [unknown suspect] at the time of the three suspect shipments, the Court cannot conclude that there is probable cause to believe that the location and identifying information of any of these other persons contains evidence of the offense." Id. at *55-56 (emphasis in original).

With respect to particularity, Magistrate Judge Fuentes emphasized that under established Supreme Court precedent, "a warrant to search a place cannot normally be construed to authorize a search of each individual in that place," and, further, "[a] warrant that meets the particularity requirement leaves the executing officer no discretion as to what to seize." Id. at *56, 58. The government argued that its third application satisfied the particularity requirement because the proposed geofences were "narrowly tailored in a manner justified by the investigation." Id. at *57. Specifically, the government argued that the proposed geofences were "constrained both geographically and temporally to the receipt and shipment of stolen prescription medication that the government is investigating." Id. at *56. But Magistrate Judge Fuentes disagreed, concluding that "the warrant here gives the officer unbridled discretion as to what device IDs would be used as the basis for the mere formality of a subpoena to yield the identifying subscriber information, and thus, those persons' location histories." In his view, "[t]his amount of discretion is too great to comply with the particularity requirement." Id. at *63.

In closing, Magistrate Judge Fuentes clarified that by denying the government's application, he did not "intend to suggest that geofence warrants are categorically unconstitutional." Id. at *64. Rather, "[e]ach specific proposed application must comply with longstanding constitutional protections of individual privacy rights, which should not be diminished by increased technical capability for intrusion, or by how effective those capabilities might be at solving crimes."