JULANDER BROWN & BOLLARD

FILE NUMBER:
3MCW01-03

June 4, 2024

Via Electronic Mail

Jenna Bulis
E-Mail: [redacted]

Re: Evidence Preservation
McNamara, et al. v. Breaking Code Silence, et al.

Dear Ms. Bulis,

I am writing to notify you that my clients, Katherine McNamara and Jeremy Whiteley, intend to file an action for malicious prosecution (hereinafter the "Litigation") in connection with the now-dismissed federal action styled *Breaking Code Silence v. McNamara, et al.,* Central District of California Case No. 2:22-cv-002052 (the "BCS Action"). If you are receiving this letter, you may either be named as a defendant in the Litigation, be a material witness in the Litigation, or possess relevant documents and electronically stored information related to the Litigation.

Please regard this letter as notice to you to preserve all electronically stored information, copies, and backups, along with any paper files which you maintain, relevant to the initiation and maintenance of the BCS Action, including privileged materials. Under both California and Federal law, you are required to preserve all electronically stored information ("ESI") in your custody and control that is relevant.

You Must Consider ESI Broadly

ESI should be afforded the broadest possible definition and includes (by way of example and not as an exclusive list) potentially relevant information electronically, magnetically or optically stored as:

- Digital communications (e.g., e-mail, voice mail, instant messaging);
- Word processed documents (e.g., Word or WordPerfect documents and drafts);
- Spreadsheets and tables (e.g., Excel or Lotus 123 worksheets);

- Accounting Application Data (e.g., QuickBooks, Money, Peachtree data files);
- Image and Facsimile Files (e.g., .PDF, .TIFF, .JPG, .GIF images);
- Sound Recordings (e.g., .WAV and .MP3 files);
- Video and Animation (e.g., .AVI and .MOV files);
- Databases (e.g., Access, Oracle, SQL Server data, SAP);
- Contact and Relationship Management Data (e.g., Outlook, ACT!);
- Calendar and Diary Application Data (e.g., Outlook PST, Yahoo, blog tools);
- Online Access Data (e.g., Temporary Internet Files, History, Cookies);
- Presentations (e.g., PowerPoint, Corel Presentations)
- Network Access and Server Activity Logs;
- Project Management Application Data;
- Computer Aided Design/Drawing Files; and,
- Back Up and Archival Files (e.g., Zip, .GHO).

Preservation Requires Immediate Intervention

You must act immediately to preserve potentially relevant ESI. Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. You must also intervene to prevent loss due to routine operations and employ proper techniques and protocols suited to the protection of ESI. Be advised that sources of ESI are altered and erased by continued use of your computers and other devices. Booting a drive, examining its contents or running any application will irretrievably alter the evidence it contains and may constitute unlawful spoliation of evidence. Consequently, alteration and erasure may result from your failure to act diligently and responsibly to prevent loss or corruption of ESI. Nothing in this demand for preservation of ESI should be understood to diminish your concurrent obligation to preserve documents, tangible things, and other potentially relevant evidence.

Suspension of Routine Destruction

You are directed to immediately initiate a litigation hold for potentially relevant ESI, documents, and tangible things, and to act diligently and in good faith to secure and audit compliance with such litigation hold. You are further directed to immediately identify and modify or suspend features of your information systems and devices that, in routine operation, operate to cause the loss of potentially relevant ESI. Examples of such features and operations include:

- Purging the contents of e-mail repositories by age, capacity or other criteria;
- Using data or media wiping, disposal, erasure or encryption utilities or devices;
- Overwriting, erasing, destroying or discarding back up media;
- Re-assigning, re-imaging or disposing of systems, servers, devices or media;
- Running antivirus or other programs affecting wholesale metadata alteration;
- Releasing or purging online storage repositories;
- Using metadata stripper utilities;
- Disabling server or IM logging;
- Executing drive or file defragmentation or compression programs;
- Turning on or failing to turn off disappearing messages in Signal;
- Uninstalling/Deleting the Signal application from your devices;
- Deleting chats, emails, etc. under the belief or assumption it is "privileged;"
- Deleting Facebook chats; and
- Deleting Facebook accounts.

Guard Against Deletion

For law firms and other businesses, you should anticipate that your clients and employees, and other persons or entities with access to the ESI may seek to hide, destroy or alter ESI. You must act to prevent or guard against such actions. This concern is not one unique to you or those associated with you. It's simply an event that occurs with such regularity in electronic discovery efforts that any custodian of ESI and their counsel are obliged to anticipate and guard against its occurrence.

Preservation in Native Form

You should anticipate that certain ESI, including but not limited to spreadsheets and databases, will be sought in the form or forms in which it is ordinarily maintained. Accordingly, you should preserve ESI in such native forms, and you should not select methods to preserve ESI that remove or degrade the ability to search your ESI by electronic means or make it difficult or burdensome to access or use the information efficiently in the litigation. You should additionally refrain from actions that shift ESI from reasonably accessible media and forms to less accessible media and forms if the effect of such actions is to make such ESI not reasonably accessible.

Metadata

You should further anticipate the need to disclose and produce system and application metadata and act to preserve it. System metadata is information describing the history and characteristics of other ESI. This information is typically associated with tracking or managing an electronic file and often includes data reflecting a file's name, size, custodian, location and dates of creation and last modification or access. Application metadata is information automatically included or embedded in electronic files but which may not be apparent to a user, including deleted content, draft language, commentary, collaboration and distribution data and dates of creation and printing. Be advised that metadata may be overwritten or corrupted by careless handling or improper steps to preserve ESI.

Servers

With respect to servers like those used to manage electronic mail (e.g., Microsoft Exchange, Lotus Domino) or network storage (often called a user's "network share"), the complete contents of each user's network share and e-mail account should be preserved. There are several ways to preserve the contents of a server depending upon, e.g., its RAID configuration and whether it can be downed or must be online 24/7. If you question whether the preservation method you pursue is one that we will accept as sufficient, please call to discuss it.

Ancillary Preservation

You must preserve documents and other tangible items that may be required to access, interpret or search potentially relevant ESI, including logs, control sheets, specifications, indices, naming protocols, file lists, network diagrams, flow charts, instruction sheets, data entry forms, abbreviation keys, user ID and password rosters or the like.

You must preserve any passwords, keys or other authenticators required to access encrypted files or run applications, along with the installation disks, user manuals and license keys for applications required to access the ESI.

You must preserve any cabling, drivers, and hardware if needed to access or interpret media on which ESI is stored.

Do Not Delay Preservation

You should not defer preservation steps if ESI may be lost or corrupted as a consequence of delay. Should your failure to preserve potentially relevant evidence result in the corruption, loss, or delay in production of evidence to which we are entitled, such failure would constitute spoliation of evidence, and we will not hesitate to seek sanctions.

Duration of Preservation Obligation

Your obligation to preserve documents and ESI will continue through the conclusion of the Litigation, including the exhaustion of all appeals. You will receive a written notice when the preservation obligation has ended.

Consequences of Non-Compliance

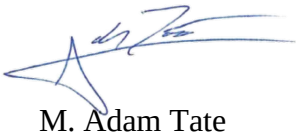
Failure to comply with this preservation notice may result in the imposition of sanctions by the court presiding over the Litigation. These sanctions may include adverse jury instructions, dismissal of claims or defenses, civil contempt, and monetary sanctions.

Confirmation of Compliance

Please confirm by June 14, 2024, that you have taken the steps outlined in this letter to preserve potentially relevant ESI and tangible documents.

If you have any questions about the scope of your preservation obligations, please feel free to contact me.

Very truly yours,



M. Adam Tate
JULANDER, BROWN & BOLLARD