DEC 8 PM 2:43

Request for Public Records

Submittal of this form is not required but it is provided for your convenience.

Contra Costa County

To Be Completed by Requester

Elijah Dominguez
Name of Requester

12/6/2017
Date

Agency/Company

Eli.dominguez1992@protonmail.ch
Email Address

700 Alhambra Ave #223
Mailing Address

N/A
Phone #

N/A
Fax #

Requested Documents/Information:
(please be as specific as possible, e.g., subject matter, key words, date range, County department(s), etc.)

See Attachment C for contra costa county sheriff department

FOR OFFICE USE ONLY

(Official Date Stamp)	(Official Date Stamp)	(Official Date Stamp)
Clerk's Initials:	Clerk's Initials:	Clerk's Initials:
Request Received	**Notification of Records Availability Given**	**Records Picked Up / Mailed / Faxed**
☐ Walk-in	☐ Immediate	☐ Picked Up
☐ Mail	☐ One Business Day	☐ Mailed
☐ Phone / Fax	☐ Other: _____	☐ Faxed
☐ Other: _____	Comment:	☐ Other: _____

Number of Copies: _____ X $____ per page = $_____ *(reference Administrative Bulletin 120 for fees)*

Computer media: = $_____

Postage: = $_____

Other: = $_____

TOTAL: = $_____

Total Money Collected $_____ **Cash / Check / Money Order**

Customer Receipt #: _____ **Cashier's Initials:** _____

Please use a separate form for each request!

Electronically Stored Information Hold/Litigation Hold and FOIA Request

I, Elijah Dominguez, in connection with Contra Costa County Department involving Officer marino spencer,and wohn kooy battle and Hughes . On September 15th, 2016, I was (cited, stopped, detained, arrested, witnessed, etc.) by Officer wohn,spencer and Marino kooy battle and Hughes I who issued a summons against me for trespassing **Battery on a Peace / Police Officer obstructing a peace officer and mayhem**

under California Penal Code Section 602 PC and penal code 203-205 and penal code pc 69 which before issuing a summons for the charges under California Penal Code Section 602 PC penal code 203-205 and penal code pc 69 The charge are pending in the Contra Costa County Superior Court for the city of Martinez

FOIA Request

Pursuant to the California Freedom of information act (FOIA) I demand that you submit the following information/documents to me: 1. Any and all videotape from every onboard camera of every police vehicle which pursued Elijah Dominguez corresponded to any incident involving trespassing on september15th 2016

2. Any and all audio tapes, audio tracks, audio recordings, or transcripts of all police radio traffic taken on september15th 2016 related to deputies marino spencer,and wohn kooy battle and Hughes and I Elijah Dominguez including but not limited to all radio traffic from the time officer I pursued I Elijah Dominguez until I was released and all communication related to I Elijah Dominguez ended (hereinafter referred to as the Dominguez incident

3. Any and all police dispatch logs related to the Dominguez incident (september15th 2016

4. A copy of the original summons for trespassing under California Penal Code Section 602 PC

5. Any and all police notices or advisories related to Elijah Dominguez held by the Martinez police department

6. Records specifically concerning deputies marino spencer,and wohn kooy battle and Hughes I kept pursuant to **SB-1286 Peace officers: records of misconduct** including without limitation any personnel records, any documents collected, created, or
maintained in connection with complaints or concerns raised about Officer marino spencer,and wohn kooy battle and Hughes behavior or conduct, and any documents collected, created, or maintained in connection with any investigations into officer marino spencer,and wohn kooy battle and Hughes behavior or conduct.

7. The number of records responsive to each of the above requests that are being withheld, and the specific basis for each such records being withheld.

Electronically Stored Information ("ESI") Hold
Litigation Hold of ESI

Additionally, Elijah Dominguez demand that you preserve all documents, tangible things and electronically stored information potentially relevant to his claims arising out of the stop on September 15th 2016 and subsequent prosecution, including but not limited to:

1. Any and all documents which describe actions taken by officer marino spencer,and wohn kooy battle and Hughes against me, Elijah Dominguez
2. 2. Any and all communications by the Martinez police department about me, Elijah Dominguez
3. 3. Any and all communications by any party concerning me, Elijah Dominguez and/or the interaction between and officer marino spencer,and wohn kooy battle and Hughes and I and/or the court and/or the Contra Costa County Attorney's office
4. 4. Any and all documents related to the prosecution of I, Elijah Dominguez
5. 5. Any and all documents related to any actions or conduct of any officers involved in my (Dominguez) stop, detention, issuance of summons, and/or prosecution;
6. 6. Internal Investigations related to the Dominguez incident
7. 7. Any discipline arising out of the Dominguez incident

As used in this demand, "you" and "your" refers to the Martinez Police Department its successors, divisions, affiliates, and its officers, directors, agents, attorneys, committees, accountants, employees, or other persons occupying similar positions or performing similar functions. You should anticipate that much of the information subject to disclosure or responsive to discovery in this matter, should the matter proceed to litigation, is stored on your current and former computer systems and other media and devices (including personal digital assistants, voice-messaging systems, online repositories and cell phones).

Electronically stored information (hereinafter "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)

- 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 effecting wholesale metadata alteration;
- Releasing or purging online storage repositories;
- Using metadata stripper utilities;
- Disabling server or 1M logging; and,
- Executing drive or file defragmentation or compression programs.

Guard Against Deletion

You should anticipate that your employees, officers or others may seek to hide, destroy or alter ESI and act to prevent or guard against such actions. Especially where company machines have been used for Internet access or personal communications, you should anticipate that users may seek to delete or destroy information they regard as personal, confidential or embarrassing and, in so doing, may also delete or destroy potentially relevant ESI. This concern is not one unique to you or your employees and officers. 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 by Imaging

You should take affirmative steps to prevent anyone with access to your data, systems and archives from seeking to modify, destroy or hide electronic evidence on network or local hard drives (such as by deleting or overwriting files, using data shredding and overwriting applications, defragmentation, re-imaging or replacing drives, encryption, compression, steganography or the like). With respect to local hard drives, one way to protect existing data on local hard drives is by the creation and authentication of a forensically qualified image of all sectors of the drive. Such a forensically qualified duplicate may also be called a bitstream image or clone of the drive. Be advised that a conventional back up of a hard drive is not a forensically qualified image because it only captures active, unlocked data files and fails to preserve forensically significant data that may exist in such areas as unallocated space, slack space and the swap file.

With respect to the hard drives and storage devices of each of the persons identified below and of each person acting in the capacity or holding the job title named below, as well as each other person likely to have information pertaining to the instant action on their computer hard drive(s), demand is made that you immediately obtain, authenticate and preserve forensically qualified images of the hard drives in any computer system (including portable and home computers) used by that person during the period from September 15th 2016

To the present and continuing, as well as recording and preserving the system time and date of each such computer.

Once obtained, each such forensically qualified image should be labeled to identify the date of acquisition, the person or entity acquiring the image and the system and medium from which it was obtained. Each such image should be preserved without alteration.

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. For electronic mail, metadata includes all header routing data and Base 64 encoded attachment data, in addition to the To, From, Subject, Received Date, CC and BCC fields.

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.

Home Systems, Laptops, Online Accounts and Other ESI Venues

Though we expect that you will act swiftly to preserve data on office workstations and servers, you should also determine if any home or portable systems may contain potentially relevant data. To the extent that officers, board members or employees have sent or received potentially relevant e-mails or created or reviewed potentially relevant documents away from the office, you must preserve the contents of systems, devices and media used for these purposes (including not only potentially relevant data from portable and home computers, but also from portable thumb drives, CD-R disks and the user's PDA, smart phone, voice mailbox or other forms of ESI storage.). Similarly, if employees, officers or board members used online or browser-based email accounts or services (such as AOL, Gmail, Yahoo Mail or the like) to send or receive potentially relevant messages and attachments, the contents of these account mailboxes (including Sent, Deleted and Archived Message folders) should be preserved.

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 10 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, other than a standard 3.5" floppy disk drive or standard CD or OVO optical disk drive, if needed to access or interpret media on which ESI is stored. This includes tape drives, bar code readers, Zip drives and other legacy or proprietary devices.

Paper Preservation of ESI is Inadequate

possession of potentially relevant ESI to preserve such ESI to the full extent of your obligation to do so, and you must take reasonable steps to secure their compliance.

System Sequestration or Forensically Sound Imaging

I removing their ESI systems, media and devices from service and properly sequestering and protecting them may be an appropriate and cost-effective preservation step. In the event you deem it impractical to sequester systems, media and devices, we believe that the breadth of preservation required, coupled with the modest number of systems implicated, dictates that forensically sound imaging of the systems, media and devices is expedient and cost effective. As we anticipate the need for forensic examination of one or more of the systems and the presence of relevant evidence in forensically accessible areas of the drives, we demand that you employ forensically sound ESI preservation methods. Failure to use such methods poses a significant threat of spoliation and data loss.

By "forensically sound," we mean duplication, for purposes of preservation, of all data stored on the evidence media while employing a proper chain of custody and using tools and methods that make no changes to the evidence and support authentication of the duplicate as a true and complete bit-for-bit image of the
original. A forensically sound preservation method guards against changes to metadata evidence and preserves all parts of the electronic evidence, including in the so-called "unallocated clusters," holding deleted files.

Preservation Protocols

I am desirous of working with you to agree upon an acceptable protocol for forensically sound preservation and can supply a suitable protocol, if you will furnish an inventory of the systems and media to be preserved. Else, if you will promptly disclose the preservation protocol you intend to employ, perhaps we can identify any points of disagreement and resolve them. A successful and compliant ESI preservation effort requires expertise. If you do not currently have such expertise at your disposal, we urge you to engage the services of an expert in electronic evidence and computer forensics. Perhaps our respective experts can work cooperatively to secure a balance between evidence preservation and burden that's fair to both sides and acceptable to the Court.

Do Not Delay Preservation

I'm available to discuss reasonable preservation steps; however, you should not defer preservation steps pending such discussions 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.

Confirmation of Compliance

Please confirm that you have taken the steps outlined in this letter to preserve ESI and tangible documents potentially relevant to this action. If you have not undertaken the steps outlined above, or have taken other actions, please describe what you have done to preserve potentially relevant evidence.

I look forward to your prompt response.

Elijah Dominguez

700 Alhambra avenue #223 martinez,ca 94553