MORRISON FOERSTER

Report of Investigative Findings and Recommendations

California Department of Justice OpenJustice Firearms Dashboard June 27-28, 2022 Exposure of Confidential Personal Data

November 30, 2022

Prepared by Morrison & Foerster LLP

Carrie H. Cohen
Brian R. Michael
Christine Y. Wong

Table of Contents

Among its critical responsibilities and mandates, the California Department of Justice (DOJ):

> *. . . manag[es] multiple data repositories that contain highly sensitive and regulated criminal justice… and personally identifiable data. The confidentiality of this data must be protected at all times to ensure the DOJ continues to meet its responsibilities as custodians and providers of this data.*

(DOJ Administrative Manual, Chapter 15, Information Technology).

Despite this directive, from June 27-28, 2022, confidential firearms-related data managed by DOJ was publicly exposed on OpenJustice, a DOJ website intended to provide the public with aggregated, anonymized criminal justice data. Specifically, for a period of less than 24 hours, public visitors to OpenJustice were able to access confidential personal information related to concealed carry weapon permit applicants and holders and other firearms-related data that could be associated with or used to identify individuals.

As detailed further in this Report of Investigative Findings and Recommendations (Report), the improper exposure of confidential personal data by DOJ, while unacceptable, was unintentional and not connected to any nefarious purpose. The investigation found that the data exposure was due to a lack of DOJ personnel training, requisite technical expertise, and professional rigor; insufficiently documented and implemented DOJ policies and procedures; and inadequate oversight by certain supervisors. This combination of factors resulted in errors, poor judgment, and missed opportunities by certain DOJ personnel, and ultimately, in DOJ's failure to meet the responsibilities with which it was entrusted as the custodian of confidential personal information.

To help restore the community's trust and confidence in DOJ's continued ability to manage and protect confidential personal data, this Report sets forth: (1) factual findings regarding the circumstances of the data exposure, and (2) recommendations to improve DOJ's handling of such data to avoid improper exposure in the future.

I. EXECUTIVE SUMMARY

A. Background

On June 27, 2022, as part of its commitment to publicly share criminal justice data in a transparent manner, DOJ published on its public-facing **OpenJustice**[1] website an interactive dashboard containing firearms-related data (the **Firearms Dashboard**). DOJ's intent was to publish only aggregated, anonymized data; DOJ personnel did not intend for confidential information that could be associated with or used to identify individuals, and that should not be publicly disclosed (**confidential personal data**[2]), to be accessible to the public on OpenJustice.

[1] An Appendix of Key Terms is attached to this Report; certain of these key terms are bolded and/or abbreviations of them are repeated herein for ease of reference.

[2] For purposes of this Report, the data that was never intended to be publicly disclosed in the dataset underlying the Firearms Dashboard, some of which could be used to identify individuals, is referred to herein as "confidential personal data." This description of "confidential personal data" is not, nor should it be understood as, the legal definition of "Personal Identifiable Information" (PII), as that term is used in other contexts. A more detailed description of the confidential personal data that was disclosed in the data exposure is set forth at Section VI.E.

The same day the Firearms Dashboard was published on OpenJustice, DOJ was alerted that confidential personal data might be publicly accessible, and an internal effort was promptly undertaken to assess whether this was true. Early the next morning, on June 28, DOJ determined that confidential personal data in an underlying dataset that was used to create the Firearms Dashboard but that was not intended for public dissemination had been accessible to the public on OpenJustice. The Firearms Dashboard promptly was taken offline and, later that same day, the entire OpenJustice website was taken offline.

Thereafter, in addition to DOJ's own efforts to address the data exposure, DOJ engaged Morrison & Foerster LLP (Morrison Foerster) in early July 2022 to conduct an independent investigation to determine the cause, nature, and scope of the public exposure of confidential personal data on the Firearms Dashboard. FTI Consulting, Inc. (FTI), a firm with forensic cyber expertise, was engaged to work at Morrison Foerster's direction and conduct a review and analysis of the data exposure.

Morrison Foerster had the mandate and autonomy to conduct an independent investigation that followed the facts and evidence wherever they led and make findings and remedial recommendations. Consistent with this mandate and autonomy, and with the full cooperation of DOJ and its personnel, Morrison Foerster conducted its investigation with FTI's assistance. The investigation included numerous interviews, collection and review of tens of thousands of documents, and a review and analysis of the computing environment used to create and publish the Firearms Dashboard.

This Report sets forth those findings and recommendations.

B. Development and Publication of the Firearms Dashboard

DOJ's California Justice Information Services Division (CJIS) provides criminal history and data to state and local law enforcement and regulatory agencies. CJIS also supports DOJ's information technology (IT) infrastructure. The Research Center is a component within CJIS that conducts criminal justice-related research and analyzes and provides data to the public and law enforcement agency partners. As part of these responsibilities, the Research Center oversees OpenJustice, a DOJ website that publishes criminal justice data in various formats, including interactive dashboards using a software program called **Tableau**.[3]

In late 2021, DOJ's Bureau of Firearms (BOF), the DOJ component within the Division of Law Enforcement that is responsible for, among other functions, issuing firearms permits, sought to make additional firearms-related data available on OpenJustice in response to increased public and media attention on and requests for such data. To that end, in late 2021 and early 2022, the Research Center undertook the creation of the Firearms Dashboard, a public-facing interactive

[3] Tableau is a commercially available software program that DOJ licensed and began using in 2019.

data display on OpenJustice, which was to include enhanced and updated firearms-related data in aggregated, anonymized form appropriate for public disclosure.[4]

A Research Center data analyst (Data Analyst-1), who had worked on other dashboards, was tasked with creating the Firearms Dashboard. Data Analyst-1 extracted a dataset from relevant DOJ-maintained databases with data related to Concealed Carry Weapon (CCW) permits, Firearms Safety Certificates (FSC), Dealer Record of Sale (DROS), and the Assault Weapons Registry (AWR). When creating this dataset, Data Analyst-1 included confidential personal data beyond what was necessary to create the intended public displays of data on the Firearms Dashboard. Contrary to established DOJ protocols, Data Analyst-1 uploaded this dataset with confidential personal data to Tableau (the **underlying dataset**). Also included in the underlying dataset was data related to Gun Violence Restraining Orders (GVRO) and the Roster of Certified Handguns, neither of which contained confidential personal data. Data Analyst-1 analyzed and organized data drawn from the underlying dataset into various aggregated, anonymized categories, including location, age, race, and gender, for publication on the Firearms Dashboard. Data Analyst-1 completed a draft of the Firearms Dashboard by mid-February 2022.

From mid-February to mid-June 2022, the Firearms Dashboard draft was reviewed by other DOJ personnel and executives who provided feedback regarding the intended public-facing visualizations, appearance, and user-experience. During these reviews, there was no substantive inquiry or discussion, however, regarding the underlying dataset and whether confidential personal data had been included in it. Nor was there any substantive inquiry or discussion regarding the configuration of Tableau security settings, which may permit or deny public access to the underlying dataset. While DOJ personnel and executives involved in the review widely understood and believed that only aggregated non-confidential data was intended to be publicly accessible on the Firearms Dashboard (and all other OpenJustice dashboards), there was no rigorous or systematic effort to confirm this was true.

The Firearms Dashboard was formally approved for publication on OpenJustice in mid-June 2022. In the early afternoon of June 27, 2022, the Firearms Dashboard was published and went live for public access.

C. Notification of Data Exposure and DOJ Review

In the early evening of June 27, 2022, the Attorney General received a direct message on his personal Twitter account from an unfamiliar sender stating that confidential personal data associated with CCW-related data was publicly accessible on the Firearms Dashboard. The Attorney General immediately notified the Chief Deputy Attorney General (CDAG), who alerted the CJIS Chief, who in turn contacted the Research Center Director. Research Center personnel promptly began to investigate this claim. Shortly thereafter, it was discovered that the Firearms Dashboard (and all other dashboards on OpenJustice) could not be accessed because the DOJ-

[4] The Attorney General and other DOJ senior executives were generally aware of the Research Center's work to update and enhance firearms-related data available to the public on OpenJustice through the creation of the Firearms Dashboard but, as described below, were not involved in the day-to-day efforts to do so.

managed servers running the Tableau software platform (the **Tableau server**) were down.[5] In response, personnel from the Application Development Bureau (ADB), a CJIS component with responsibility for DOJ's IT infrastructure, and other DOJ personnel undertook efforts to resolve the server outage.

That same evening, while efforts were underway to resolve the server outage, Data Analyst-1, together with the Research Center Director, probed the Firearms Dashboard to determine if there was any way public visitors to OpenJustice could access confidential personal data. Data Analyst-1 repeatedly assured and demonstrated (erroneously, as was later determined) for the Research Center Director that only aggregated, anonymized data was displayed and available to the public. Data Analyst-1 also showed the Research Center Director the underlying dataset not intended for public display, whereby the Research Center Director learned for the first time that Data Analyst-1 had unnecessarily included confidential personal data associated with CCW-related data in the underlying dataset. Data Analyst-1 repeatedly assured the Research Center Director, however, that the underlying dataset could not be publicly accessed. Nevertheless, the Research Center Director directed Data Analyst-1 to replace the underlying dataset with one that did not include any confidential personal data. Data Analyst-1 indicated that a new dataset could be ready that same evening.

The Research Center Director then reported to the CJIS Chief that Data Analyst-1 had included confidential personal data in the underlying dataset for the Firearms Dashboard but that such data was not publicly accessible based both on Data Analyst-1's assurances and the Research Center Director's and Data Analyst-1's review of the Firearms Dashboard. Relying on these assurances, but without ordering further investigation or seeking assistance from ADB or other DOJ personnel with technical expertise, the CJIS Chief assured the CDAG that no confidential personal data was publicly accessible on the Firearms Dashboard. The CJIS Chief, however, never informed the CDAG that Data Analyst-1 had included confidential personal data in the underlying dataset and that such data had not yet been removed.

At the same time that Research Center personnel were probing the claim that confidential personal data was publicly accessible on the Firearms Dashboard, ADB personnel, acting at the direction of the ADB Director, probed the cause of the Tableau server outage, along with personnel from the Technology Services Bureau (TSB), another CJIS component. The ADB and TSB personnel concluded that the outage was due to inadequate server storage capacity. Due to poor communication, however, ADB and TSB personnel addressing the Tableau server outage were not focused on or were unaware of the claim regarding public access to confidential personal data. They, along with the ADB Director and the CJIS Chief, did not recognize a possible connection between the claim that confidential personal data was publicly accessible (including available for download) on the Firearms Dashboard and the Tableau server outage.[6]

[5] While the Tableau server was down, the OpenJustice website was accessible but visitors could not view or access the dashboards.

[6] This investigation found that the outage was caused by the creation of temporary files using up space on the Tableau server as a result of public visitors seeking to download the underlying dataset with confidential personal data.

Later that evening, relying on the assurances from the Research Center Director that confidential personal data could not be publicly accessed on the Firearms Dashboard, the CJIS Chief unilaterally decided that when the Tableau server was restored, the Firearms Dashboard (with the same underlying dataset containing confidential personal data) should go live again. The CJIS Chief also decided that, due to the late hour and resulting increased risk of error, Data Analyst-1 should wait until the following morning to upload a new underlying dataset that did not contain any confidential personal data.

Late in the night of June 27, the ADB team was able to increase the storage capacity of the Tableau server and the Firearms Dashboard was brought back online with the original underlying dataset, as directed by the CJIS Chief. Early the next morning, June 28, Data Analyst-1 uploaded a new underlying dataset to the Tableau server that did not include any confidential personal data associated with CCW-related data, thereby replacing the initial underlying dataset. The FSC, DROS, and AWR-related data, however, was not updated in that new underlying dataset.[7]

Shortly thereafter, that same June 28 morning, DOJ personnel learned that DOJ had received additional reports that confidential personal data was publicly accessible the previous night and early morning *after* the Tableau server was restored and the Firearms Dashboard went live again. Accordingly, the Research Center Director and Data Analyst-1, with the assistance of the ADB Director, further probed the Firearms Dashboard. They then discovered, for the first time, a means by which public visitors could access the underlying dataset. Upon this discovery, the Research Center Director informed the CJIS Chief that confidential personal data likely had been available to the public on the Firearms Dashboard. The CJIS Chief then alerted the CDAG.

Immediately after being informed by the CJIS Chief that confidential personal data could have been accessed by the public on the Firearms Dashboard, the CDAG directed that the Firearms Dashboard be taken down, which occurred shortly before noon Pacific Time on June 28. Later that same day, at the CDAG's direction, the entire OpenJustice website was taken offline.

D. Nature and Extent of Exposed Data

The investigation confirmed that confidential personal data in the underlying dataset associated with CCW, FSC, DROS, and AWR-related data was publicly accessible on the Firearms Dashboard from June 27-28 for a period of less than 24 hours.[8] More specifically, confidential personal data from CCW, FSC, DROS, and AWR-related data became available when the Firearms Dashboard first went live in the early afternoon of June 27, until the Tableau server went down in the early evening; and again after the Tableau server was restored later in the night on June 27. CCW-related confidential personal data was available until the early morning of June 28 when the underlying dataset was replaced with an updated dataset that did not include the CCW-related confidential personal data. FSC, DROS, and AWR-related confidential

[7] The investigation determined that confidential personal data *also* was contained in the underlying FSC, DROS, and AWR-related data but that Data Analyst-1 either was unaware of or forgot this fact and thus focused only on removing the CCW-related confidential personal data from the underlying dataset.

[8] As explained above, and more fully below, confidential personal data was not included in the underlying dataset for GVRO and was never part of the Roster of Certified Handguns data.

personal data was available, for a slightly longer period of time, until the Firearms Dashboard was taken offline shortly before noon Pacific Time on June 28.

The investigation also confirmed that, within the underlying dataset for the Firearms Dashboard, only confidential personal data associated with CCW-related data, which included names of individuals, could be used to independently identify those individuals. As such, in total, confidential personal data for approximately 192,000 individuals was exposed in connection with CCW-related data on the Firearms Dashboard. None of the other exposed confidential personal data contained information that could be used to independently identify individuals.[9]

Further, the investigation confirmed that the Firearms Dashboard's underlying dataset containing confidential personal data was downloaded approximately 2,734 times, in full or in part, across 507 unique IP addresses.[10] The investigation could not accurately determine the number of public visitors who may have only viewed, but did not download, the underlying dataset. The decision by the CJIS Chief to go live again with the Firearms Dashboard the night of June 27 after the Tableau server was restored proved to be a compounding error. The majority of these downloads occurred *after* the Firearms Dashboard became accessible again on OpenJustice late in the night on June 27 until the Firearms Dashboard was taken down the next morning at the CDAG's direction.

E. Tableau Security Settings

Based on the review and analysis of the computing environment used to create and publish the Firearms Dashboard, the investigation found that the underlying dataset – and the confidential personal data unnecessarily included therein – was publicly accessible due to an erroneous configuration of Tableau security settings that allowed access to the underlying dataset.

More specifically, Tableau has a hierarchy of security settings at three levels – "project," "workbook," and "sheet." Project level settings are administrator-level settings to which Data Analyst-1 did not have access and that were managed by an internal DOJ "Tableau Team" within ADB. The project level settings were configured, apparently unbeknownst to the Tableau Team despite its administrator role, to allow Data Analyst-1 the ability to configure the security settings at the workbook and sheet levels. Consistent with informal written guidance provided by former Research Center colleagues, Data Analyst-1 configured the Tableau security settings at the workbook level seeking to deny public access to the underlying dataset. But, to effectively deny public access to the underlying dataset, Data Analyst-1 *also* needed to configure the security settings at the sheet level. Data Analyst-1 claimed to be unaware of this additional step and thus did not take that step, which resulted in sheet-level settings not being properly configured to deny public access to the underlying dataset. As a result of not configuring the Tableau security settings to deny public access at *both* the workbook *and* sheet levels, and unbeknownst to Data Analyst-1 (and apparently to other DOJ personnel who were involved in

[9] Even though confidential personal data associated with the FSC, DROS, and AWR-related data was exposed, as discussed more fully below, no individual names were disclosed with this data, and therefore there is limited additional risk from cross-correlation.

[10] An IP address generally corresponds to a unique device's connection to the Internet. The number of unique IP addresses corresponds approximately to the number of unique individuals that downloaded data.

the creation and review of the Firearms Dashboard), there remained active functionality on the Firearms Dashboard that enabled public visitors to access the underlying dataset.

Ultimately, the investigation found that the conduct of Data Analyst-1 and the Tableau Team, and that of certain DOJ supervisors, when taken together, unintentionally – but unacceptably – allowed public access to the underlying dataset with confidential personal data. Namely, when the Firearms Dashboard was published on June 27: (1) the underlying dataset created and uploaded by Data Analyst-1 to the Tableau server unnecessarily contained confidential personal data, in contravention of DOJ policy and practice; and (2) Tableau security settings were improperly configured to allow public access to this confidential personal data.

F. Key Findings

As described further in this Report, the investigation found the following:

1. Policies and Training for Handling Confidential Personal Data

- DOJ has generally applicable policies and training regarding handling and protection of confidential personal data and DOJ personnel receive annual training regarding the importance of safeguarding such data.

- Although DOJ has well-established policies and training regarding handling and protection of confidential personal data, there was a lack of clearly documented, delineated, or centralized oversight of information security related to OpenJustice dashboards.

- While the DOJ Research Center has detailed draft policies that set forth key concepts and controls for handing confidential personal data, it does not have a formal written policy or role-specific training regarding how confidential personal data should be handled in connection with dashboards on OpenJustice.

2. Creation and Development of the Firearms Dashboard

- Although internal approval is required for Research Center personnel to access firearms-related databases, once granted, there was inconsistent and minimal oversight and instruction regarding how to extract and handle such data.

- Contrary to DOJ formal and informal policies regarding the protection of confidential personal data and Research Center protocol and practice, Data Analyst-1 unnecessarily uploaded to Tableau confidential personal data without the knowledge of other DOJ personnel, including Research Center supervisors.

- There is no evidence that Data Analyst-1's inclusion of confidential personal data in the underlying dataset was done with nefarious intent or that any DOJ personnel intended for the public release of confidential personal data.

- While Data Analyst-1 acted without nefarious intent, Data Analyst-1 was inattentive to established policies and procedures, lacked necessary appreciation for security risks, and had insufficient knowledge of Tableau security settings; Data Analyst-1 also had inadequate training and supervision.

- While the Firearms Dashboard was subject to multiple levels of internal review during its development and before it was published, these reviews were not sufficiently documented, systematic, or rigorous, and did not include confirmation that there was no confidential personal data in the underlying dataset and/or accessible to the public.

3. Publication of the Firearms Dashboard on June 27, 2022

- DOJ personnel – both those responsible for creating and publishing the Firearms Dashboard and those responsible for Tableau server administration – did not receive necessary training on Tableau (and were not directed to do so by supervisors), including on best practices or security settings configuration; the same DOJ personnel did not seek any assistance with Tableau security settings configuration (and were not directed to do so by supervisors) in connection with the Firearms Dashboard, despite having access to Tableau technical support and other resources.

- At the time the Firearms Dashboard was published on OpenJustice, the Tableau security settings were improperly configured such that the public was able to view and download the underlying dataset containing confidential personal data; there is no evidence, however, that this configuration was done intentionally or that any DOJ personnel were aware of this security failure.

- The timing of publication of the Firearms Dashboard was not driven by the U.S. Supreme Court's *Bruen* decision although it was recognized by DOJ executives that whenever that decision was issued, there likely would be heightened interest in firearms-related data.

4. DOJ Discovery of June 27-28 Data Exposure

- After receiving a direct message via social media on June 27 stating that confidential personal data was accessible to the public on the Firearms Dashboard, the Attorney General promptly asked the CDAG to determine whether the claim was true.

- While probing the validity of the claim that confidential personal data was accessible to the public on the Firearms Dashboard, CJIS personnel learned that: (1) the Tableau server was down but did not connect that fact to potential

exposure and download of confidential personal data; and (2) confidential personal data had been uploaded unnecessarily by Data Analyst-1 to the Tableau server as part of the underlying dataset even though it was not intended to be visible to the public.

- Based on repeated assurances by the Research Center Director (based on discussions with Data Analyst-1) that confidential personal data could not be accessed by the public, the CJIS Chief assured the CDAG of the same; the CJIS Chief, however, never informed the CDAG that confidential personal data had been unnecessarily included in the underlying dataset.

- Without conducting further investigation or consulting with the CDAG, the CJIS Chief directed that the Firearms Dashboard with the underlying dataset containing confidential personal data should go live again after the Tableau server was restored the night of June 27.

- Although DOJ personnel promptly investigated the report of a possible data exposure, these efforts were undermined by lack of effective coordination and communication between various CJIS components, an overall lack of technical expertise, and the failure of DOJ personnel, including certain supervisors, to more closely probe the cause of the server outage and to verify assertions by Data Analyst-1 that confidential personal data was not publicly accessible.

- It was not discovered that the public could view the underlying confidential personal data until the morning of June 28; DOJ personnel's prior assurances to the contrary were based on an incomplete review of the Firearms Dashboard active functionality and an erroneous understanding of Tableau security settings.

5. Scope of Data Exposed on the Firearms Dashboard

- The underlying dataset for the Firearms Dashboard that was publicly accessible contained confidential personal data associated with CCW, FSC, DROS, and AWR-related data; confidential personal data was not included in the underlying GVRO-related data and was never part of the Roster of Certified Handguns data.

- Within the underlying dataset for the Firearms Dashboard, only CCW-related data could be used to independently identify individuals (because the fields exposed included associated names); analysis revealed that none of the other data in the underlying dataset contained information that could be used to independently identify individuals. In total, drawing from the CCW-related data, confidential personal data was exposed on the Firearms Dashboard for approximately 192,000 individuals.

- Even though confidential personal data was exposed in the FSC, DROS, and AWR-related data, the risk from such exposure is limited because the data cannot be used to independently identify individuals (because the fields exposed did not have an associated individual name or other identifier). Further, cross-correlation analysis identified only one possible means of enriching the data that presented limited additional risk; other enrichment of the data required unverifiable assumptions.

- Confidential personal data was available for a period of time that was less than 24 hours: from when the Firearms Dashboard first went live on June 27 until the Tableau server was down and, again, after the Tableau server was restored until it was taken offline on June 28.

- The exposed underlying dataset with confidential personal data was viewed by members of the public and downloaded, in full or in part, approximately 2,734 times across 507 unique IP addresses.

- The decision by the CJIS Chief to go live again with the Firearms Dashboard the night of June 27 after the Tableau server was restored proved to be a compounding error. The vast majority of public downloads of confidential personal data occurred during this latter period of time until the Firearms Dashboard was taken down the next morning at the CDAG's direction.

6. Analysis of Additional OpenJustice Dashboards

- Although confidential personal data was publicly accessible on the Firearms Dashboard, the investigation did not find that confidential personal data was publicly accessible on any other OpenJustice dashboard.

G. Timeline of Key Events[11]

Fall 2021-Early 2022	Research Center and BOF discuss updating firearms data on OpenJustice, and Research Center begins work on Firearms Dashboard, including Data Analyst-1's extraction of firearms-related data from DOJ databases.
Jan.-Mar. 14, 2022	Research Center drafts and revises Firearms Dashboard, including feedback obtained during review by other DOJ personnel and executives.
Mar. 17-June 16, 2022	Required approvers review Firearms Dashboard with final approval granted on June 16.
June 21-23, 2022	Press release for Firearms Dashboard drafted and approved; publication delayed due to other press-related issues.

[11] All times provided in this Report are approximate and in Pacific Time.

June 27, 2022	• 12:30 p.m.: Firearms Dashboard published on OpenJustice; press release issued. • 6:15-6:30 p.m.: Attorney General receives message via social media claiming that confidential personal data is available on Firearms Dashboard; notifies DOJ executives of claim and directs for it to be reviewed; CDAG instructs senior DOJ personnel to review claim. • 6:30 p.m.: DOJ personnel begin to investigate claim and learn that OpenJustice is down due to server outage. • 7:00-9:00 p.m.: Research Center Director learns confidential personal data associated with CCW-related data was included unnecessarily by Data Analyst-1 in underlying dataset used to create Firearms Dashboard (but accepts assurances from Data Analyst-1 during review of the Firearms Dashboard that it was not publicly accessible). This is communicated to CJIS Chief, who does not communicate it to CDAG. • 9:30 p.m.: At CJIS Chief's direction, Firearms Dashboard brought back online with original underlying dataset containing confidential personal data. • 10:00 p.m.: Data Analyst-1 and Research Center Director review the Firearms Dashboard after its restoration and again assure CJIS Chief that underlying dataset was not publicly accessible; CJIS Chief directs that underlying dataset containing confidential personal data can be replaced the next morning.
June 28, 2022	• 6:30 a.m.: Data Analyst-1 replaces confidential personal data associated with CCW-related data in underlying dataset on Firearms Dashboard (but not confidential personal data associated with DROS, FSC, and AWR-related data, which DOJ had not yet detected). • 8:00-11:30 a.m.: DOJ personnel review additional claims that confidential personal data is accessible on Firearms Dashboard and determine that confidential personal data in the underlying dataset had been available on the public-facing Firearms Dashboard; after being informed, the CDAG directs Firearms Dashboard be taken down. • 11:45 a.m.: Firearms Dashboard taken down from OpenJustice. • 9:00 p.m.: Full OpenJustice website taken offline.

II. SCOPE AND METHODOLOGY OF INVESTIGATION

As noted above, Morrison Foerster was hired in July 2022 by DOJ to conduct an independent investigation into the public exposure of confidential personal data arising from the publication of the Firearms Dashboard on DOJ's OpenJustice website. Morrison Foerster had the mandate and autonomy to follow the facts and evidence wherever they led and to make independent findings and recommendations. The investigation was wholly directed and conducted by Morrison Foerster and was not limited by any DOJ personnel or third parties. DOJ cooperated fully and provided Morrison Foerster with prompt access to documents, employees, and all other information sought.

The investigative team has significant experience conducting complex internal and government-related investigations. The Morrison Foerster team is led by former federal and state prosecutors with expertise in investigating and responding to data and cybersecurity breaches as well as conducting independent reviews for public-facing matters.[12] FTI was engaged as a forensic cyber expert to work at Morrison Foerster's direction and conduct an analysis of the data exposure. FTI was selected for its well-established reputation for integrity and independence; in-depth forensic, data, and cybersecurity analysis abilities; and extensive experience in handling sensitive data exposures. FTI's team also was led by former federal government officials and law enforcement agents.

Morrison Foerster's engagement focused on developing an understanding of the causes and circumstances of the June 27-28 data exposure. Accordingly, a comprehensive audit of the entirety of DOJ's information security systems, policies, protocols, and practices was not conducted. Even though the data exposure was associated only with the Firearms Dashboard, the investigation included a review of OpenJustice to determine if additional confidential personal data may have been exposed publicly on other OpenJustice dashboards.

This Report is based on Morrison Foerster's independent investigation and review conducted with the assistance of FTI. This Report does not seek to catalog all information learned from interviews, document review, forensic examination, or other investigative efforts; rather, this Report presents a summary and analysis of key facts and relevant information learned during the course of this investigation, as well as Morrison Foerster's findings and recommendations.

III. BACKGROUND

A. Overview of OpenJustice and Dashboards

OpenJustice is a DOJ website that publishes criminal justice information and data for the public, including through interactive online dashboards that contain charts and other visualizations. After OpenJustice was launched by DOJ in 2015, the California State Legislature unanimously passed in 2016 the OpenJustice Data Act, Assembly Bill (AB) 2524 (the OpenJustice Data Act of 2016). The OpenJustice Data Act of 2016 mandated DOJ to make certain criminal justice

[12] Morrison Foerster associates Vanshika Vij and Karen Leung also were core members of the Morrison Foerster team and, along with other Morrison Foerster associates, paralegals, and staff, they were integral to the investigation and preparation of this Report.

data available for the public on OpenJustice and to update that data annually in order to facilitate accountability and transparency in California's criminal justice system.

At the time OpenJustice was first launched in 2015, it provided data from DOJ's statewide repository of criminal justice datasets. Later, interactive dashboards were added that spotlighted key criminal justice indicators with user-friendly visualizations. Over time, DOJ created and published additional dashboards on OpenJustice to provide greater public access to demographic and statistical information, including by displaying aggregated, anonymized data on a variety of criminal justice topics, such as arrests, adult and juvenile probation, use of force, specific crimes (*e.g.*, homicides, hate crimes), and firearms. By aggregating large amounts of data, data analysts are able to identify and show trends while avoiding the disclosure of personal identification of any individuals. As such, the OpenJustice dashboards were intended to display only aggregated, anonymized data; confidential personal data was never intended to be publicly accessible.

B. Overview of Firearms Data on OpenJustice

In order to increase transparency and help implement informed data-driven public policy, firearms sales and ownership data first was published by DOJ on OpenJustice on October 12, 2016. Three separate firearms-related dashboards were initially published, drawing from the following two underlying datasets: (1) Dealer Record of Sale (DROS),[13] which contained information from applications submitted by prospective firearms purchasers to licensed firearms dealers (one of the dashboards); and (2) Gun Violence Restraining Orders (GVRO), which contained information from court orders that prohibit specific individuals from owning or possessing a firearm or ammunition (two of the dashboards). These three firearms-related dashboards displayed changes in firearms sales over time, types of firearms purchased, sales and transfers of pre-owned firearms, and numbers of GVROs issued. The dashboards were periodically updated to provide current data and information.

In late 2021, due to an increase in public interest in firearms data – including data requests from researchers, journalists, legislators, and other government officials – DOJ began working on a new firearms-related dashboard, *i.e.*, the Firearms Dashboard. This Firearms Dashboard was intended to achieve the following objectives: (1) consolidate various firearms data and supplementary information (including data from the three existing firearms-related dashboards described above); (2) introduce data from additional firearms-related datasets; and (3) update existing data to include the 2021 reporting year. To aid in displaying the data on the Firearms Dashboard in an accessible format, DOJ used Tableau, a data visualization software platform (described further below).

In addition to data from DROS and GVRO, the Firearms Dashboard included information from the following additional four sets of data:

- Concealed Carry Weapons (CCW): applicants for concealed carry weapon permits;
- Firearms Safety Certificates (FSC): holders of firearms safety certificates;

[13] DROS-related data comes from four different data sources within DOJ. In this Report, DROS-related data collectively refers to data from all four sources.

- Assault Weapons Registry (AWR): registered assault weapons; and

- Roster of Certified Handguns: a list of handguns, including make and model information, approved to be sold in California.

The Firearms Dashboard also included certain demographic information – *e.g.*, race, gender, age range, county/geography – for the purposes of filtering and sorting aggregated data.[14] Further, it provided new links to supplemental resources, such as reports, applications, legal information, and "Frequently Asked Questions," among other enhancements.

C. Overview of June 27-28, 2022 Data Exposure

On Monday, June 27, 2022, at 12:30 p.m., the Firearms Dashboard was published by DOJ and went live on OpenJustice. Later that day, the Attorney General received messages on his Twitter account stating that confidential personal data was accessible to the public on the Firearms Dashboard. The Attorney General promptly notified the Chief Deputy Attorney General (CDAG), who in turn instructed the Chief of the California Justice Information Services Division (CJIS), which oversaw the operation of OpenJustice, to investigate the issue. Upon looking into the claim, DOJ personnel learned that the Tableau server hosting the public-facing Firearms Dashboard (and other dashboards) was offline and the public could no longer access OpenJustice and thus could not view the dashboards. DOJ personnel sought to restore the Tableau server while simultaneously seeking to determine whether confidential personal data was, in fact, publicly accessible on the Firearms Dashboard.

In probing whether confidential personal data was available on the Firearms Dashboard, Research Center personnel came to the conclusion that evening – learned later to be incorrect – that there was no means by which the public could access any such data on the Firearms Dashboard. The Research Center Director also learned that Data Analyst-1 had uploaded an underlying dataset that included confidential personal data associated with CCW-related data to the Tableau server hosting the Firearms Dashboard, in contravention of DOJ policies and Research Center protocols. The Research Center Director directed that a new underlying dataset that did not contain any such confidential personal data be created and uploaded by Data Analyst-1 to the Tableau server. Ultimately, on the basis of assurances given by Data Analyst-1 to the Research Center Director that confidential personal data could not be publicly accessed on the Firearms Dashboard, which were, in turn, conveyed by the Research Center Director to the CJIS Chief, the CJIS Chief directed that the Firearms Dashboard should go live that night once the server outage was resolved. The CJIS Director further directed that, given the late hour and resulting increased risk of error, the underlying dataset need not be replaced until the next morning.

Later that night, the Tableau server hosting the public-facing Firearms Dashboard (and other dashboards) was brought back online and the Firearms Dashboard again was accessible to the

[14] *See* Section VI.E. *infra* for a more detailed discussion of the data included on the Firearms Dashboard.

public on OpenJustice. At that time, DOJ personnel continued to believe confidential personal data had not previously been, and was still not, publicly accessible.

On Tuesday, June 28, at 6:30 a.m., Data Analyst-1 replaced the underlying dataset with one that did not include the confidential personal data associated with the CCW-related data. Shortly thereafter, DOJ personnel became aware of additional reports from the public that confidential personal data was publicly accessible on the Firearms Dashboard. While conducting further investigation into these reports, DOJ personnel determined that, in fact, the public had been able to view and download confidential personal data from the Firearms Dashboard since it was first launched the day before and, again, after the Tableau server was restored and the Firearms Dashboard was brought back online. DOJ promptly took the Firearms Dashboard offline and, later that day, took down the entire OpenJustice website so that no dashboards or other data could be accessed by the public. While public access to OpenJustice has since been restored, all of the interactive dashboards on OpenJustice, including the Firearms Dashboard, remain offline and inaccessible to the public today.

D. Overview of DOJ Response and Investigation

Following the events of June 27-28, 2022, DOJ engaged IDX, a digital privacy protection and data breach response services company, to conduct and manage a notification process for individuals likely affected by the data exposure. As part of this effort, notification letters were sent on or about July 8 to approximately 218,000 potentially impacted individuals. Those letters provided, among other things, information regarding free credit monitoring and identity theft protection services and a call center to answer questions.

DOJ also created a website dedicated to informing the public about the June 27-28 data exposure, which remains online today.[15] Through this website, DOJ provides updates regarding the data exposure and information about available resources, including identity protection services.

As detailed above, DOJ also promptly engaged Morrison Foerster and FTI to conduct an independent investigation of the June 27-28 data exposure, including to review and determine how it occurred and the nature and extent of the data exposure.

IV. DETAILS OF INVESTIGATION

Morrison Foerster's investigation included the following: (1) collection and review of tens of thousands of DOJ documents, including relevant policies and procedures, vendor contracts, emails, and text messages; (2) FTI's review of DOJ applications, systems, and servers; and (3) interviews by Morrison Foerster of 32 DOJ current and former employees, some of whom were interviewed multiple times.

[15] The website is available at https://oag.ca.gov/dataexposure.

A. FTI Review

In order to ascertain the potential nature, scope, and extent of the confidential personal data exposed on the Firearms Dashboard, FTI conducted a detailed technical analysis and review of the software and servers used by DOJ personnel to create and publish the dashboards on OpenJustice. FTI's review also included an assessment of whether other dashboards published on OpenJustice prior to June 28, 2022 contained confidential personal data that may have been publicly accessible.

1. Review of Tableau Environment

FTI received an image of the Tableau production server that DOJ personnel had taken of the Firearms Dashboard on the day it launched on June 27.[16] FTI also created a model of the Tableau production environment to test the Tableau security settings (further explained below).

2. Analysis of Exposed Data

FTI's review included analysis and identification of the type and amount of data downloaded from the Firearms Dashboard while confidential personal data was publicly accessible on June 27-28. To conduct this analysis, FTI reviewed and analyzed DOJ network logs covering the period from June 26 to 28.[17]

The network log files provided the names of underlying datasets, including self-describing file names, *e.g.*, CCW, FSC, or AWR. For non-descriptive file names, FTI estimated the contents of the file by comparing its download size to a dataset's known file size. By analyzing the file names and the file sizes, FTI was able to identify successful downloads of the underlying dataset for the Firearms Dashboard (as opposed to summary data, such as visuals that did not include confidential personal data).

Through this analysis, FTI was able to determine the approximate total number of downloads of the underlying dataset containing confidential personal data and the total number of unique IP addresses that downloaded the underlying dataset containing confidential personal data.

3. Analysis of Additional OpenJustice Dashboards

In addition to the Firearms Dashboard, FTI reviewed and analyzed other dashboards that were or may have at some point been published on OpenJustice to assess whether confidential personal data may have been publicly accessible from those dashboards. For this review and analysis, FTI also relied on the Tableau production server image from June 27.

---

[16] As a general matter, OpenJustice operates on several servers that run Tableau software and are maintained by DOJ in two computing environments, namely, staging and production. The staging environment is inaccessible to the public and is where OpenJustice dashboards are created and reviewed by DOJ personnel. The production environment houses dashboards that are published on OpenJustice and accessible to public visitors.

[17] The network logs are DOJ IT records containing details related to website visitors and data downloads by the public (including the visitor's IP address, the specific site visited, and other digital artifacts).

B. Document Review

Numerous documents were collected for the investigation, consisting of email and electronic files and other materials from approximately 21 DOJ custodians, as well as mobile device data, Microsoft Teams data, policies and procedures, and other documents.[18] A comprehensive list of key search terms related to the data exposure and the Firearms Dashboard was developed and applied to these materials, resulting in more than 40,000 relevant documents that were reviewed by Morrison Foerster.

C. Interviews

Morrison Foerster conducted 40 interviews of 32 DOJ personnel, including one employee who left DOJ during the pendency of the investigation (for reasons unrelated to the data exposure) but voluntarily continued to cooperate.

At the direction of Morrison Foerster, a member of the FTI team also participated in some interviews. Further, DOJ engaged counsel from another law firm to advise on employment matters arising from the data exposure. For efficiency purposes, counsel from that law firm participated in certain interviews.

Several DOJ interviewees exercised their right to be accompanied by a representative, including in one instance by individual counsel, while other DOJ interviewees voluntarily opted to proceed without any representative. All DOJ personnel for whom interviews were requested agreed to be interviewed and answered every question asked of them.

Where this Report refers to collective knowledge of DOJ personnel, that knowledge is limited to those DOJ personnel who were interviewed and the review of the relevant documents. During the course of the investigation, Morrison Foerster also considered witness credibility based on interviewees' biases, experience, demeanor, and potential motivations, as well as the statements of other interviewees and the review of other relevant materials.

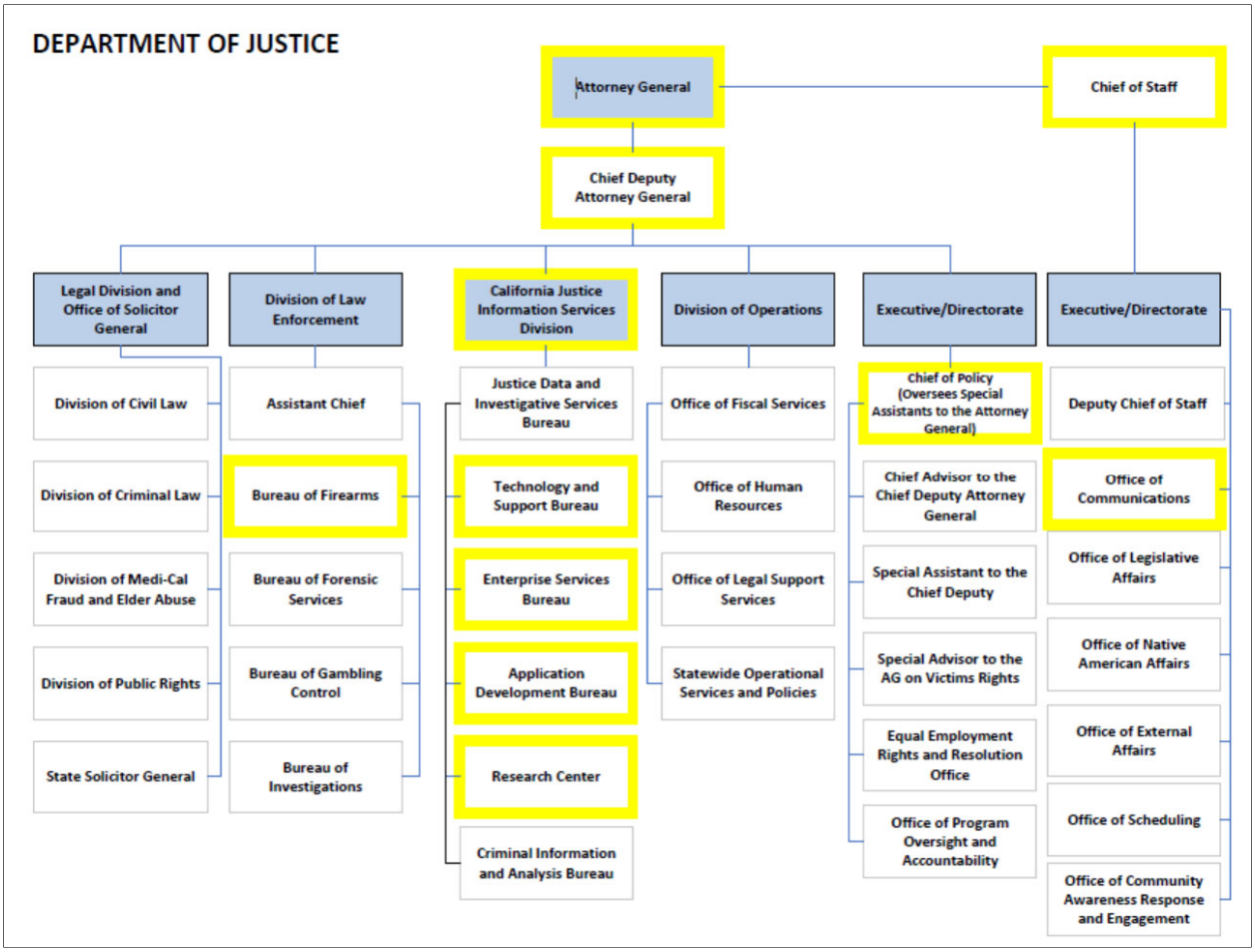
V. DOJ STRUCTURE AND RELEVANT COMPONENTS

A. California Department of Justice

The California Department of Justice (DOJ) is a law enforcement agency with statewide jurisdiction under the elected leadership of the Attorney General. DOJ also serves as counsel for many California state agencies and maintains a repository of criminal justice information, among other responsibilities. The Chief Deputy Attorney General (CDAG) reports to the Attorney General and oversees the following five divisions: (1) Legal Division and Office of the Solicitor General; (2) Division of Law Enforcement; (3) Division of Operations; (4) Executive/ Directorate; and (5) California Justice Information Services Division (CJIS). The Chief of Staff also reports to the Attorney General and oversees parts of the Executive/Directorate Division that performs non-legal functions (*e.g.,* Office of Communications).

[18] Promptly after the data exposure, DOJ took appropriate steps to preserve relevant data.

An organizational chart of DOJ is provided below, with entities relevant for this Report highlighted and further described below.



California Department of Justice Organizational Chart as of July 2022

1. Executive/Directorate Division

The Executive/Directorate Division (also referred to as the Executive Programs Division), consolidates functions not directly related to litigation or law enforcement. This Division has several components, which report to either the CDAG or the Attorney General's Chief of Staff. These include the following:

a. Office of Communications

The Office of Communications (referred to as "Communications") coordinates, among other things, media coverage to publicize departmental actions and legal developments and inform the public of the Attorney General's views on significant legal and public policy issues. The Office of Communications is led by a Director who reports to the Chief of Staff.

b. Special Assistants to the Attorney General

Special Assistants to the Attorney General are attorneys who serve on the Attorney General's executive staff and assist on a variety of legal matters as well as represent the Attorney General as members of, or liaisons to, certain State boards and commissions. The Special Assistants to the Attorney General report to the Chief of Policy, who reports to the CDAG.

2. Division of Law Enforcement

The Division of Law Enforcement's mission is to enhance public safety by conducting regulatory oversight, criminal investigations, and forensic analysis of evidence for criminal proceedings, as well as enhance safety within California. The Division consists of several components, one of which is the Bureau of Firearms (BOF). BOF's mission includes education, regulation, and enforcement actions regarding the manufacture, sale, ownership, testing, and transfer of firearms.

As part of its responsibilities, BOF issues permits to possess, manufacture, or sell certain firearms; facilitates firearms-related background checks; processes assault weapon registrations; administers firearms certificate programs, including safety certificates; oversees certain aspects of out-of-state delivery, sale, and transfer of firearms; and oversees certain aspects of gun shows. BOF processes information related to firearms licensing and permits, which is maintained in DOJ firearms-related databases.

3. California Justice and Information Services Division

The mission of the California Justice and Information Services Division (CJIS) is to provide accurate, timely, and comprehensive criminal history and analysis data to its client agencies, which include local police and sheriffs' departments, district attorneys, and local and state regulatory agencies. CJIS also supports DOJ's Information Technology (IT) infrastructure. CJIS consists of several bureaus described further below. CJIS is led by a Chief who reports to the CDAG.

a. Research Center

The Research Center conducts a wide variety of research and data-related services for DOJ and the public, such as empirical studies and literature reviews; qualitative reviews; statistical modeling; and recidivism reporting. Among its responsibilities, the Research Center works with various CJIS components and other DOJ database owners[19] to gather data for dashboard visualizations on OpenJustice. Certain of these dashboards are updated annually in compliance with California law.[20]

[19] Database "owner" as used in this Report refers to the DOJ department or other organization that receives, collects, generates, and/or maintains the original underlying criminal justice data.
[20] As noted above, the OpenJustice Data Act of 2016 (AB 2524) requires DOJ to make certain criminal justice data publicly available on OpenJustice and to update that data annually.

The Research Center is led by a Director, who oversees a team of Supervisors, Data Specialists, and Data Analysts. Research Center personnel were primarily responsible for the development of the Firearms Dashboard.

b. Application Development Bureau

ADB is responsible for designing, implementing, and maintaining DOJ's statewide criminal justice IT systems, supporting the Division of Law Enforcement's applications, and providing analytical reporting and information services.

Certain ADB personnel provide internal DOJ technical support for Tableau (the Tableau Team), among other responsibilities. The Tableau Team has a Lead Administrator and a backup administrator. These administrators are supervised by an Information Technology Supervisor II, who is in turn supervised by an Information Technology Manager I. The Tableau Team is part of the Statistical & Integrated Reporting Services Unit, which provides support for data requests. In addition to other responsibilities, the Tableau Team manages and maintains the Tableau server, works with Research Center personnel to publish OpenJustice dashboards, and meets regularly with a technical account manager from Tableau.

ADB has multiple branches and units to support firearms applications and systems that contain firearms-related data, including the Managed Application Support Systems (MASS) Section. MASS oversees several functions, including the unit responsible for granting DOJ employees access to firearms databases as necessary.

MASS also oversees the Web Development Team (the Web Team). The Web Team supports DOJ's public and internal websites and applications, including conducting regular reviews for security vulnerabilities. Among its responsibilities, the Web Team ensures that OpenJustice is functional. The Web Team was not involved in the creation of the Firearms Dashboard except to provide Roster of Certified Handgun-related data, which did not contain confidential personal data, and a member of the Web Team provided technical assistance on June 27 to prepare the Firearms Dashboard for publication.

c. Enterprise Services Bureau

The Enterprise Services Bureau (ESB) is responsible for DOJ IT contracts and purchasing, project oversight and coordination, and the provision and maintenance of IT systems and related services to DOJ statewide. ESB also provides enterprise support for DOJ's computing, applications, and shared services environments associated with DOJ programs and law enforcement agency partners to ensure technical solutions meet state and federal information security requirements.

ESB houses a Cybersecurity Branch, which includes an Information Technology Manager II (ITM II) who is responsible for establishing organization-wide policies and standards for DOJ IT security. The ITM II serves as the DOJ Information Security Officer and manages network security development, review, and approval of certain IT systems.

ESB personnel, including the ITM II, were not involved in the creation or launch of the Firearms Dashboard or DOJ personnel's response to the June 27-28 data exposure.

d. Technology Services Bureau

The Technology Services Bureau (TSB) is responsible for infrastructure and software used to support DOJ and is responsible for ensuring all systems are available to DOJ's law enforcement community and DOJ personnel. TSB also designs, coordinates, installs, and provides 24-hour support for communication applications, server infrastructure, and networks used by DOJ, state criminal justice agencies, and national criminal justice systems.

B. DOJ's Use of Tableau

1. Background

Tableau is a company that creates and licenses commercially available software for data manipulation and visualization applications. DOJ began using Tableau in 2019 to help create user-friendly OpenJustice dashboards.

More specifically, DOJ licenses two Tableau products: Tableau Desktop and Tableau Server.[21] As used by the Research Center, Tableau Desktop provides a computing environment that allows data analysts to produce data visualizations in the form of interactive dashboards, while Tableau Server provides staging and production environments (respectively, **Tableau staging environment** and **Tableau production environment**). In the Tableau staging environment, DOJ personnel are able to test and review the dashboards. In the Tableau production environment, DOJ personnel can publish finalized dashboards to OpenJustice for public viewing.

Tableau provides DOJ with a set number of licenses that are assigned to DOJ personnel so they are able to use the software. Research Center personnel who were assigned Tableau licenses used Tableau Desktop to upload underlying datasets and create dashboards with visualizations of data drawn from these datasets. When these dashboards were ready for review, they were uploaded to Tableau Server, from which they were reviewed in the staging environment and, once approved, transferred to the production environment to be made available to the public on OpenJustice.

As noted above, there was an internal Tableau Team within ADB that was responsible for administering, configuring, and managing the Tableau server and supporting DOJ personnel who used Tableau.[22] DOJ also received support directly from Tableau through a technical account manager. The Tableau Team served as the primary DOJ point of contact with Tableau, holding regular weekly meetings with the Tableau technical account manager during which the Tableau Team was apprised of technical changes and other relevant developments and could raise issues or questions. Research Center personnel were invited to and attended some of these meetings.

[21] "Tableau Server" is a specific product name, as compared to the more generalized term "Tableau server" as defined and used in this Report.
[22] The TSB also provides Tableau server infrastructure support.

2. Use of Tableau to Create, Review, and Publish the Firearms Dashboard

Research Center personnel used Tableau Desktop to conduct necessary analysis and grouping of the data to create visualizations for the Firearms Dashboard. When the visualizations were complete, and a "draft" version of the Firearms Dashboard was ready, the Research Center stored the draft Firearms Dashboard on the Tableau staging environment, which was only accessible to DOJ personnel. The draft Firearms Dashboard then was tested and reviewed as it would appear to public visitors once published, initially by Research Center and BOF personnel, and later by other DOJ personnel and executives.

Once this review process was complete, and the draft Firearms Dashboard was revised accordingly, it was formally approved by DOJ executives and uploaded to the Tableau production environment for publication on OpenJustice.

VI. FACTUAL FINDINGS

A. Policies and Training for Handling Confidential Personal Data

Key Findings

- DOJ has generally applicable policies and training regarding handling and protection of confidential personal data and DOJ personnel receive annual training regarding the importance of safeguarding such data.
- Although DOJ has well-established policies and training regarding handling and protection of confidential personal data, there was a lack of clearly documented, delineated, or centralized oversight of information security related to OpenJustice dashboards.
- While the DOJ Research Center has detailed draft policies that set forth key concepts and controls for handing confidential personal data, it does not have a formal written policy or role-specific training regarding how confidential personal data should be handled in connection with dashboards on OpenJustice.

DOJ's policy on handling confidential personal data is set forth in the "Information Technology" chapter of the State of California Department of Justice Administrative Manual ("DOJ Manual"), a Department-wide manual. The DOJ Manual explains that DOJ is responsible for, among other things:

> . . . manag[ing] multiple data repositories that contain highly sensitive and regulated criminal justice… and personally identifiable data. The confidentiality of this data must be protected at all times to ensure the DOJ continues to meet its responsibilities as custodians and providers of this data.

(DOJ Administrative Manual, Chapter 15, Information Technology).

DOJ personnel who handle "confidential information," including confidential personal data maintained or stored on the DOJ network, are directed to take precautions to protect such information on a "need-to-know, right-to-know" basis. For example, before any record is

released publicly, the DOJ Manual requires that all confidential, sensitive, or personal information in the record be removed, redacted, or masked. Managers are required to ensure that employees adhere to these procedures.[23] DOJ personnel also are required to take an annual online security training that includes instruction on handling sensitive information. DOJ personnel involved in the Firearms Dashboard completed this required training and were uniformly aware of and understood that confidential personal data must be actively protected from public disclosure. They also were aware that maintaining confidentiality and having proper safeguards and controls in place to secure such information is a top priority.

Research Center personnel in particular handle confidential personal data in the normal course of their job responsibilities, which include responding to frequent internal and external data requests. For example, the Research Center has experience suppressing low counts in publicly released data (*i.e.,* masking small sub-populations of people or events using statistical techniques to ensure that specific individuals cannot be identified from aggregated data). The Research Center, however, does not have formal, finalized written policies regarding the handling of confidential personal data or the release of data on OpenJustice.[24]

There are two *draft* Research Center policy documents that were created in or around 2019: the "Research Center Data Request Policies" (the Draft Data Governance Manual) and the "Data Access and Analysis Section Desk Manual" (the Draft Desk Manual).[25] These draft policies primarily address data requests from external researchers as responding to these requests is part of the Research Center's responsibilities. Neither of these draft policies was finalized nor formally adopted. While not entirely clear, it appears the drafts never were formally adopted because other work demands drew attention elsewhere and because there was turnover of the DOJ personnel who had primarily been involved in the effort to create these materials. Multiple Research Center employees, however, were aware of these draft policies and were familiar with or involved in drafting some of the procedures within them. Research Center personnel involved in the creation of OpenJustice dashboards also expressed widespread knowledge and understanding of and adherence to the data security principles espoused within these draft policies. But there did not appear to be uniform familiarity with, or mandated use or reliance on, the entirety of the draft policies themselves.

Both the Draft Data Governance Manual and the Draft Desk Manual contain instructions on the proper handling of confidential personal data, including procedures for sharing it with external researchers. Consistent with the DOJ Manual, these draft procedures for sharing confidential personal data with external researchers generally require that confidential personal data be shared only on a "need-to-know, right-to-know" basis. Research Center personnel understood that the draft policies and procedures, although not explicitly stated therein, also apply to DOJ personnel

[23] Regarding data security, Information Technology Support Services is responsible for reviewing desktop and mobile computing configurations and specifications of equipment and software. However, the DOJ employee who is the designated owner of a record, including electronic records, is considered ultimately responsible for defining security precautions that will protect the security, integrity, and appropriate level of confidentiality of the record.
[24] The CJIS Policies and Procedures Manual (2019) does not address polices or practices related to handling confidential personal data.
[25] The Research Center has three other Desk Manuals that cover particular types of data, including Controlled Substance Utilization Review and Evaluation System (CURES) data, GVRO data, and Stop Data Collection System (SDCS) data. This Report refers to these manuals collectively as the "Draft Desk Manual."

handling confidential personal data in other contexts, including for publication on OpenJustice dashboards.

The Draft Desk Manual requires employees to check whether it is appropriate to provide confidential personal data in response to an inquiry and sets forth detailed instructions tailored to specific datasets for data extraction, cleaning, and validation. Research Center personnel involved in the creation of OpenJustice dashboards confirmed that although the Draft Desk Manual is not a formal policy document, Research Center personnel treat it as such and regularly rely on it when handling external data requests.

Among other directives, the Draft Data Governance Manual includes a draft policy on the release of Stop Data Collection System (SDCS) data on the Racial and Identity Profiling Act (RIPA) dashboard (RIPA Dashboard) on OpenJustice. This policy prohibits certain data elements containing sensitive information from being included in the underlying data in the OpenJustice RIPA Dashboard and directs that those data elements be removed from the dataset before the RIPA Dashboard is uploaded to OpenJustice. Research Center personnel acknowledged that personnel who create and manage OpenJustice dashboards are expected to be mindful of and adhere to data handling principles outlined in the draft SDCS policy even when working with datasets for different OpenJustice dashboards, including the Firearms Dashboard.

Despite these policy directives, multiple DOJ personnel of varying seniorities and from multiple DOJ components asserted that they did not have final oversight of the transfer, handling, uploading, or publication of underlying datasets on OpenJustice, nor did they know for certain who had such final oversight, including for the Firearms Dashboard. Although the CJIS Chief acknowledged that, broadly speaking, the role of Chief bore ultimate responsibility for content on OpenJustice because it was managed and maintained by CJIS components, the CJIS Chief also noted that the Chief role oversees approximately 1,200 CJIS employees and their activities. Ultimately, DOJ personnel were unable to identify who, on a day-to-day basis, bore specific responsibility or authority over information security as it relates to OpenJustice and the dashboards published on OpenJustice. DOJ personnel also were unable to identify any formal, finalized documented policies or centralized procedures that specifically address information security for OpenJustice or the dashboards published on OpenJustice.

B. Creation and Development of the Firearms Dashboard

Key Findings:

- Although internal approval is required for Research Center personnel to access firearms-related databases, once granted, there was inconsistent and minimal oversight and instruction regarding how to extract and handle such data.
- Contrary to DOJ formal and informal policies regarding the protection of confidential personal data and Research Center protocol and practice, Data Analyst-1 unnecessarily uploaded to Tableau confidential personal data without the knowledge of other DOJ personnel, including Research Center supervisors.
- There is no evidence that Data Analyst-1's inclusion of confidential personal data in the underlying dataset was done with nefarious intent or that any DOJ personnel intended for the public release of confidential personal data.
- While Data Analyst-1 acted without nefarious intent, Data Analyst-1 was inattentive to established policies and procedures, lacked necessary appreciation for security risks, and had insufficient knowledge of Tableau security settings; Data Analyst-1 also had inadequate training and supervision.
- While the Firearms Dashboard was subject to multiple levels of internal review during its development and before it was published, these reviews were not sufficiently documented, systematic, or rigorous, and did not include confirmation that there was no confidential personal data in the underlying dataset and/or accessible to the public.

1. Background of the Firearms Dashboard

In late 2021, BOF discussed with the Research Center the need to create a new updated firearms dashboard to better respond to increased public interest in firearms-related data and the high volume of Public Records Act (PRA) requests.[26] BOF asked the Research Center to create a new firearms-related dashboard that would update and consolidate the firearms-related data already available on OpenJustice and provide additional information, including CCW-related data. Accordingly, in late 2021 and early 2022, the Research Center set out to create the Firearms Dashboard. While the Attorney General and other DOJ executives broadly were aware that the Research Center was updating and enhancing the firearms-related data available to the public on OpenJustice, they were not involved in the day-to-day efforts to create the Firearms Dashboard.

2. Extraction and Use of Firearms-Related Data for the Firearms Dashboard

To access firearms-related data stored in a centralized system at DOJ, a requestor must first obtain approval to do so from BOF and such approval is specific to the data requested. Once approval is granted, ADB personnel within the Firearms and Enterprise Systems Branch[27] facilitate technical access. Requestors typically receive data from ADB personnel, while in some

[26] The California Public Records Act, Government Code Sections 6250-6277, requires the disclosure of certain government records upon request.

[27] The Firearms and Enterprise Systems Branch is an ADB component managed by an ITM II and supports applications and systems that contain firearms-related data.

instances, requestors are granted direct, read-only access which enables them to extract an entire dataset or a subset with defined fields.

A Research Center research data analyst (Data Analyst-1), who had previously created data visualizations using Tableau for other OpenJustice dashboards, was tasked with primary responsibility for creating the Firearms Dashboard and working with BOF to identify the firearms-related data that would be included on it. Research Center colleagues who worked with Data Analyst-1 on the Firearms Dashboard uniformly described Data Analyst-1 as intelligent, hard-working, and professional.

While Data Analyst-1 had a background in research and running statistical analyses, Data Analyst-1 essentially learned "on the job" how to use Tableau to prepare the design, narrative, and detailing of the dashboards; Data Analyst-1 never received or was directed by supervisors to take any formal Tableau training. In fact, none of the Research Center personnel who used Tableau, including Data Analyst-1, received or were directed by supervisors to take any formal DOJ-sponsored or required training on how to use Tableau. Research Center personnel also did not receive any specific guidance on Tableau best practices or security settings configuration from the Tableau technical account manager or DOJ's Tableau Team. Research Center personnel relied principally on informal written guidance that was documented and passed on to them from prior Research Center personnel who had used Tableau. The Research Center personnel responsible for creating Tableau dashboards for OpenJustice, on their own accord, also sought out and took a limited amount of online Tableau training sessions. Some Research Center personnel recalled asking for formal DOJ-sponsored training, but it was never provided.

To create the underlying dataset that would form the basis of the Firearms Dashboard, and with the approval of the Directors of both the Research Center and BOF, Data Analyst-1 was granted access to firearms-related databases in order to download data. Once such access was granted, Data Analyst-1 developed and ran queries to identify, gather, and pull specific data, including CCW-related data. For this data, the queries Data Analyst-1 used resulted in the collection of a broad array of data fields that included confidential personal data, such as, first and last name, home address, and date of birth. Similarly, Data Analyst-1 collected confidential personal data associated with FSC, DROS, and AWR-related data. The extraction of much of this confidential personal data, however, was not necessary to display the intended visualizations on the Firearms Dashboard.

Indeed, according to Research Center supervisors, it was standard operating procedure communicated to Research Center personnel that no more data than is necessary for a research project should be maintained and handled, even on secure DOJ servers (*e.g.*, "need-to-know, right-to-know"). Data Analyst-1, however, claimed this was not communicated nor did Data Analyst-1 have such an understanding. Data Analyst-1 also claimed that the initial extraction of data for the Firearms Dashboard, including the confidential personal data, was intentional because it was appropriate to extract more data than was necessary at the outset of a project in order to be prepared to address questions that may arise or to make modifications or adjustments to the underlying dataset without having to extract additional data from the firearms-related databases. The investigation, however, revealed no contemporaneous written record addressing why Data Analyst-1 felt it was appropriate to extract this confidential personal data. Moreover,

Data Analyst-1 acknowledged that there was never any need to extract individual names to create the underlying dataset.

In contrast to the CCW, FSC, DROS, AWR-related data to be used for the Firearms Dashboard, Data Analyst-1 did not extract the data to be used for the Firearms Dashboard displays regarding GVRO or the Roster of Certified Handguns. Instead, Data Analyst-1 received data from the Web Team related to the Roster of Certified Handguns,[28] which did not include confidential personal data, and received an aggregated GVRO data file from the California Restraining and Protective Order System (CARPOS), from which confidential personal data was already removed.

According to Data Analyst-1, for previous Research Center projects, including the creation of other OpenJustice dashboards, Data Analyst-1 typically relied on queries run by other Research Center personnel or received a dataset from the data "owners" rather than extracting it from the relevant DOJ database. Apparently, the Firearms Dashboard was the first time Data Analyst-1 was responsible for directly extracting a dataset from a DOJ database, which also was an atypically large volume of data to be extracted. Prior to undertaking this effort, Data Analyst-1 claimed to have not received guidance or direction from Research Center supervisors or colleagues, or from any BOF personnel, regarding the nature of information to be extracted from the firearms-related databases, nor did Data Analyst-1 seek any such guidance. Data Analyst-1's direct supervisor claimed to have directed Data Analyst-1 to only pull data limited to what was needed for the Firearms Dashboard, although there is no written record of such instruction and Data Analyst-1 did not recall having been so instructed. Data Analyst-1's direct supervisor also never took steps to review the underlying dataset itself or otherwise confirm that the data extracted by Data Analyst-1 excluded unnecessary confidential personal data.

When extracting the data from the firearms-related databases, Data Analyst-1 created a list of firearms-related data that BOF proposed to update and include on OpenJustice. Thereafter, when compiling the underlying dataset, Data Analyst-1 conducted data analysis and organization for the Firearms Dashboard, for example, suppressing low counts (*i.e.,* masking small sub-populations of people or events using statistical techniques to ensure that specific individuals cannot be identified from aggregated data). At no time during this process, however, did Data Analyst-1 take any additional precautions to segregate or otherwise safeguard the confidential personal data that Data Analyst-1 had extracted from the firearms-related databases, nor was Data Analyst-1 explicitly instructed to do so by anyone. Indeed, Data Analyst-1 never thought to take any additional precautions to segregate or otherwise safeguard the confidential personal data because, according to Data Analyst-1, the datasets were being maintained on internal DOJ servers, which was a secure environment for handling sensitive data.

In addition, Data Analyst-1 did not consider the underlying dataset that Data Analyst-1 had extracted from the firearms-related databases, which included confidential personal data, to be any more sensitive than other non-public data that Data Analyst-1 previously had handled for other Research Center projects. In Data Analyst-1's view, all such data is sensitive and should be securely and carefully handled consistent with DOJ protocols, and any and all confidential data should not be publicly disclosed.

[28] Roster of Certified Handguns information is also available to the public on other parts of DOJ's website.

There is no evidence that Data Analyst-1's inclusion of confidential personal data in the underlying dataset uploaded to the Tableau server was done with nefarious intent or that any DOJ personnel intended for the public release of confidential personal data.

3. Design of the Firearms Dashboard

The Firearms Dashboard was intended to display data on OpenJustice in various visualizations, such as interactive pie and bar charts, that would be appropriate for public viewing (*i.e.*, that did not include any confidential personal data). While OpenJustice dashboards draw data from an underlying dataset to create external-facing visualizations, not all data categories in an underlying dataset may be needed for a specific visualization on the dashboard. In those situations, and even though not intended for use or public view, the data that is not relied on for the visualization still remains in the underlying dataset on Tableau.

Data Analyst-1 uploaded the underlying dataset containing confidential personal data for the Firearms Dashboard to Tableau Desktop. There, Data Analyst-1 developed visualizations intended to aggregate the data (*i.e.*, show data trends without displaying confidential personal data) for display on the Firearms Dashboard available for public viewing on OpenJustice. To create these visualizations, Data Analyst-1 used some, but not all, of the categories of data in the underlying dataset. For example, while the "date of birth" field was used by Data Analyst-1 to calculate an individual's age (*i.e.*, to see a data visualization of the age range breakdown of individuals with CCW permits), the name and street address fields were not relied on when creating such visualizations for the Firearms Dashboard. As noted above, Data Analyst-1 claimed always to have known there was confidential personal data in the underlying dataset that Data Analyst-1 had uploaded to Tableau; Data Analyst-1 also acknowledged, however, that much of this data – *e.g.,* full names – was never necessary for the data visualizations that were created for the Firearms Dashboard.

In mid-February 2022, Data Analyst-1 completed an initial "draft" version of the Firearms Dashboard using Tableau Desktop. Data Analyst-1 uploaded this draft Firearms Dashboard to the Tableau staging environment. When finalizing the draft Firearms Dashboard for publication, Data Analyst-1 relied on written step-by-step instructions regarding how to upload and publish data to the Tableau production environment, including the configuration of Tableau security settings. These instructions were set forth in an informal process document that had been created by former Research Center personnel who previously had used Tableau to create dashboards on OpenJustice. In following these steps, Data Analyst-1 never sought (nor was directed by supervisors to seek) additional guidance or assistance from the ADB Tableau Team or from Tableau technical support to confirm that the underlying dataset would not be publicly accessible. The draft Firearms Dashboard included the underlying dataset, which, as noted above, included confidential personal data, although it was not intended for public view.

4. Review and Approval of the Firearms Dashboard

Between March and June 2022, the Firearms Dashboard underwent multiple levels of internal review by DOJ personnel, as well as a formal approval process, as described more fully below.

a. Research Center Review and Feedback

While Data Analyst-1 was creating the Firearms Dashboard using Tableau Desktop, Data Analyst-1's direct supervisor and other Research Center colleagues provided informal reviews of the substance and format. Data Analyst-1 routinely sought such input, feedback, and guidance from supervisors and colleagues regarding the data to be publicly displayed, the visualizations, the user-experience, various features and functionality, and other related matters. Data Analyst-1 did not, however, seek any review of or guidance regarding, or have any detailed discussions with anyone, regarding the contents of the underlying dataset or the Tableau security settings that would be configured to protect it. Nor is there a written record of any such guidance or direction being provided by supervisors or colleagues in connection with the Firearms Dashboard.

Further, it does not appear that any additional steps were taken by Data Analyst-1's supervisors to verify that there was no confidential personal data in the underlying dataset. Both the Research Center Director and Data Analyst-1's direct supervisor acknowledged reviewing draft versions of the Firearms Dashboard; these reviews, however, did not include discussion or consideration of the contents of the underlying dataset or configuration of the Tableau security settings intended to prevent the underlying dataset's public exposure. The Research Center Director relied on the presumption that Data Analyst-1 and Data Analyst-1's direct supervisor took necessary steps to assure that confidential personal data was not in the underlying dataset or otherwise accessible to the public. According to the Research Center Director, doing so fell squarely within the responsibilities of Data Analyst-1's direct supervisor. The direct supervisor claimed, however, that a review of the underlying dataset was beyond a reasonable level of expected supervision since it should have been well-known to Data Analyst-1, based on prior discussions and well-established DOJ policies and procedures, that unnecessary confidential personal data should not be included in the underlying dataset. Further, because much of the data was not necessary for the Firearms Dashboard visualizations, there was no reason, according to Data Analyst-1's direct supervisor, to even contemplate that confidential personal data was in the underlying dataset.

The Research Center Director also believed that Data Analyst-1 and Data Analyst-1's direct supervisor were responsible for doing a systematic review of the features and functionality that would be available to the public. But, again, it was believed at the time by Data Analyst-1's direct supervisor that there was no confidential data in the underlying dataset and, therefore, in the direct supervisor's view, any systematic review or testing of every single Firearms Dashboard feature and function for this purpose was unnecessary and impractical.

Other Research Center personnel also reviewed the draft Firearms Dashboard in the Tableau staging environment, which previewed what the public would see once the Firearms Dashboard was published on OpenJustice. At no time during these reviews was it observed by any Research Center personnel that confidential personal data was in the underlying dataset or that the underlying dataset (and the confidential personal data contained therein) would be publicly accessible. According to Data Analyst-1's direct supervisor, a typical review of an OpenJustice dashboard in the Tableau staging environment included spot-checking features, such as whether

the "Download" button on the toolbar was "grayed out," *i.e.*, inactive.[29] Data Analyst-1's direct supervisor, however, did not recall specifically whether or not the download button was in fact observed to be inactive on the draft Firearms Dashboard. Data Analyst-1's direct supervisor also stated that because Tableau staging environment settings are set separately from production environment settings (*i.e.*, when a dashboard is in draft form being reviewed internally as compared to when it is in final published form accessible by the public), it is possible for certain features and functionality to appear active in the Tableau staging environment that ultimately will be inactive when the finalized dashboard is later published on OpenJustice.

Ultimately, although it was widely understood by Research Center personnel that only aggregated non-confidential personal data would be displayed publicly on the Firearms Dashboard, there was no systematic effort to test all of the functionality and features on the draft Firearms Dashboard to verify that there was no public access to the underlying dataset or any other confidential personal data. Data Analyst-1 explained that doing so would have been too time consuming and laborious given the available resources and numerous other work demands. Data Analyst-1 further explained that such an effort was perceived as unnecessary because Data Analyst-1 believed at the time, but never took appropriate steps to confirm, that the public could not access the underlying dataset, including the confidential personal data therein, because of how Data Analyst-1 had configured the security settings on Tableau.[30] Data Analyst-1's supervisors similarly explained that they always presumed, and also never took appropriate steps to confirm, that the underlying dataset did not include confidential personal data. As a result, neither Data Analyst-1 nor Data Analyst-1's supervisors believed they had any reason to verify beyond the superficial review described above whether confidential personal data would be publicly accessible on the Firearms Dashboard.

b. Other DOJ Review and Feedback

During the Firearms Dashboard drafting process, Data Analyst-1 also conferred with BOF personnel regarding the underlying firearms-related data that would be used to create the Dashboard. Data Analyst-1 met with several BOF personnel to discuss the draft Firearms Dashboard and to give them the opportunity to review the underlying dataset. During this review process, it does not appear that BOF personnel observed the confidential personal data in the underlying dataset, nor raised any questions about how Data Analyst-1 had extracted the data, what data was in the underlying dataset, or how that data had been safeguarded.

Other DOJ personnel also reviewed the draft Firearms Dashboard. Specifically, the Research Center conducted five demonstrations between mid-February and mid-March 2022, during which the draft Firearms Dashboard was presented via video conference for review and feedback. Numerous invitations were extended and shared among DOJ personnel to attend these demonstrations, including with supervisors and personnel from BOF and the Research Center;

[29] As discussed further below, by default, Tableau dashboards have a toolbar at the top or bottom of the dashboard with a "Download" button that allows the download of various dashboard categories, including data. If the "Download" button was grayed out, it would be inactive and public visitors would not be able to access the dataset underlying the dashboard. If the "Download" button was not grayed out, visitors could select the link and access the underlying dataset.

[30] The Tableau security settings set by Data Analyst-1 are further discussed *infra* at section VI.C.2 (Tableau Security Settings).

personnel from Communications, the Office of Community, Awareness, Response, and Engagement, the Office of External Affairs, and the Office of Legislative Affairs; the Chief of Policy; and a Special Assistant to the Attorney General. While not all invitees attended a demonstration, which were typically led by Data Analyst-1, DOJ personnel in each of the relevant DOJ components participated. In response to the demonstrations, participants provided feedback regarding the visualizations, appearance, and the user-experience, but there was no feedback or discussion regarding how the data was extracted from DOJ databases, the contents of the underlying dataset, the configuration of Tableau security settings, or whether confidential personal data could be downloaded and, if so, what steps had been taken to ensure that such data would not be publicly accessible. While DOJ personnel involved in these reviews of the Firearms Dashboard (and all other OpenJustice dashboards) widely understood and believed that only aggregated non-confidential data was accessible to the public on OpenJustice, there was no systematic effort or discussion to confirm if this belief was accurate.

According to other DOJ personnel who were involved in reviewing the Firearms Dashboard, it was their collective belief at the time that any concerns related to confidential personal data would have already been addressed by Research Center personnel who were more directly responsible for creating the Firearms Dashboard. Further, at no time during these internal reviews and demonstrations were DOJ personnel asked or directed, nor did they seek on their own, to conduct a systematic review or testing of all of the features and functionalities of the draft Firearms Dashboard to verify that confidential personal data was not publicly accessible.

c. Formal Approval Process

After the internal reviews of the draft Firearms Dashboard were complete and revisions were made by Data Analyst-1,[31] in mid-March 2022, a more formal approval process for the publication of the Firearms Dashboard was undertaken. This process included sending approvers a link to access and review the draft Firearms Dashboard still housed in the Tableau staging environment, after which approvers would complete an approval form, called a "JUS-128 form." The JUS-128 form is a standard DOJ approval form for OpenJustice that describes the information to be published on OpenJustice and that is required to be executed by multiple signatories.

Before signing the JUS-128 form, several of the approvers conducted a final review of the draft Firearms Dashboard that was focused primarily on visual display and user experience. Several approvers also focused on compliance with certain regulations, including those related to budget and DOJ's operational capacity, as well as consistency with public messaging of the Attorney General's priorities and compliance with certain ethics regulations. Other approvers did not conduct further review but instead relied on their prior review during a demonstration of the draft Firearms Dashboard and/or the review and approval of their colleagues or subordinates.

For the draft Firearms Dashboard, all required signatures were sought and provided: the Research Center Director (March 17), CJIS Chief (April 4), Chief of Division of Operations (April 4), a representative of the Government Law Section (April 6), Director of

[31] As discussed above, the requested changes only related to visualizations, appearance, functionality, and the user-experience.

Communications representative (April 8), a Special Assistant to the Attorney General (June 7), and the CDAG (June 16). The delay between April and when the final two signatures were provided in June was attributable to internal discussions led by a Special Assistant to the Attorney General around re-designing the visuals for the Firearms Dashboard consistent with what were perceived as improved and more user-friendly visuals deployed in another dashboard. Ultimately, it was decided that the re-design of the Firearms Dashboard visuals would take too much time and the final two approvals were provided without further redesign or changes.

After the Firearms Dashboard was formally approved, a Special Assistant to the Attorney General briefed the Attorney General regarding its forthcoming publication.[32] The Attorney General understood that updated and enhanced firearms data would be publicly available on the Firearms Dashboard, but in a manner that protected confidential personal data in full compliance with DOJ policy and the law regarding the disclosure of such data.

C. Publication of the Firearms Dashboard on June 27, 2022

Key Findings:

- DOJ personnel – both those responsible for creating and publishing the Firearms Dashboard and those responsible for Tableau server administration – did not receive necessary training on Tableau (and were not directed to do so by supervisors), including on best practices or security settings configuration; the same DOJ personnel did not seek any assistance with Tableau security settings configuration (and were not directed to do so by supervisors) in connection with the Firearms Dashboard, despite having access to Tableau technical support and other resources.
- At the time the Firearms Dashboard was published on OpenJustice, the Tableau security settings were improperly configured such that the public was able to view and download the underlying dataset containing confidential personal data; there is no evidence, however, that this configuration was done intentionally or that any DOJ personnel were aware of this security failure.
- The timing of publication of the Firearms Dashboard was not driven by the U.S. Supreme Court's *Bruen* decision although it was recognized by DOJ executives that whenever that decision was issued, there likely would be heightened interest in firearms-related data.

1. Publication to OpenJustice

As discussed above, the Research Center's initial goal was to publish the Firearms Dashboard in April 2022, concurrent with an annual release of other data, but final approval to publish the Firearms Dashboard did not occur until June 16. By that time, there were discussions among DOJ executives regarding trying to publish the Firearms Dashboard before the expected forthcoming decision by the U.S. Supreme Court in *New York State Rifle & Pistol Ass'n v.*

[32] To date, the Attorney General has never spoken with Data Analyst-1 and, accordingly, never spoke to Data Analyst-1 during the time Data Analyst-1 was working on the Firearms Dashboard. The Attorney General also was not involved in the Firearms Dashboard review process nor was his formal approval required prior to publication.

Bruen, a Second Amendment case related to firearms laws in New York State, because of the resulting likely increase in public interest in firearms-related data.[33]

On June 16, when final approval was received for the Firearms Dashboard, members of the Research Center, BOF, Communications, and a Special Assistant to the Attorney General discussed how quickly the Firearms Dashboard could be published. The Research Center confirmed that the Firearms Dashboard could be published within several hours of receiving the direction to do so. The Communications team requested a background memorandum from the Research Center summarizing the Firearms Dashboard so it could draft an accurate press release. This information was provided to the Communications team on June 21.

Around the same time the press release was being drafted, on June 23, the U.S. Supreme Court issued its decision in *Bruen*. Because DOJ was busy responding to *Bruen*, as well as to the U.S. Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization* issued the next day, a Communications team member decided, in consultation with a Special Assistant to the Attorney General, to finalize the press release announcing the Firearms Dashboard the following week.

On the morning of June 27, DOJ personnel confirmed that the Firearms Dashboard was ready to be published and could be done so concurrent with the press release. After checking with Data Analyst-1, the Research Center Director confirmed that the Firearms Dashboard would be ready for publication that day. The Research Center Director then directed Data Analyst-1 and other Research Center personnel to publish it that day. During the next few hours, Data Analyst-1 worked with a member of the ADB Web Team to prepare the Firearms Dashboard for publication.

The Firearms Dashboard was published and went live on OpenJustice on Monday, June 27 at 12:30 p.m.[34] At that time, all DOJ personnel involved in its creation and publication uniformly believed that only non-confidential data was publicly accessible. In actuality, however, the confidential personal data in the underlying dataset uploaded to Tableau by Data Analyst-1 was publicly accessible, as described further below.

The investigation did not uncover any evidence that the timing of the publication of the Firearms Dashboard was driven by a nefarious intent or was personally or politically motivated in any way; rather, it was drafted and published to meet anticipated heightened public interest in firearms-related data. Also, as discussed further below, there is no evidence that Data Analyst-1 or any other DOJ personnel intended to disclose publicly, or were aware of the potential exposure of, confidential personal data when the Firearms Dashboard was published.

[33] Data Analyst-1 was not aware of the *Bruen* decision until after the June 27-28 data exposure and neither the Research Center Director nor Data Analyst-1 were involved in these discussions.

[34] This time is estimated based on revisions made to the Firearms Dashboard in the Tableau production environment and unique external IP address access to the Firearms Dashboard.

2. Tableau Security Settings

As described in more detail below, the investigation found that DOJ personnel within the Research Center and ADB did not properly configure the Tableau security settings for the Firearms Dashboard.

Security permissions settings on Tableau dashboards may be set at three different levels: "project," "workbook," and "sheet." These security settings need to be properly configured either at the project level, or at the workbook *and* sheet level, to allow or deny public access to the underlying dataset.

If not properly understood, coordinated, or configured, Tableau security settings can override one another, which can have unintended consequences. As more fully described below, at the time the Firearms Dashboard was published on June 27, the Tableau security settings at the project level were configured by the Tableau Team to grant Data Analyst-1 the ability to configure them at the workbook and sheet; and Data Analyst-1 incorrectly did so by setting them properly *only* at the workbook level but not at the sheet level too, thereby allowing the public access to the underlying dataset containing confidential personal data.

a. Tableau Structure and Security Settings

A Tableau project is a folder that contains at least one Tableau file, called a workbook. A workbook includes an underlying dataset and the visualizations created from that dataset. Within a workbook, content may be organized or segregated into sheets. A Tableau dashboard refers to one or more sheets prepared for presentation.

At the project level, a Tableau user with administrator rights[35] has the ability to configure security settings for all projects or, in the alternative, can allow non-administrator users of Tableau, such as Research Center personnel creating dashboards, to configure those settings themselves within individual workbooks. Accordingly, the Tableau Team, who had Tableau administrator rights, could have managed and maintained responsibility for all OpenJustice dashboard security settings at the project level and not allowed this responsibility to reside with Research Center personnel at the workbook level. In other words, as administrators, the Tableau Team could have ensured that security settings at the project level precluded public access to the underlying dataset for any workbook or the corresponding sheets.

The project-level security settings, however, were configured such that Research Center personnel – including Data Analyst-1 when creating the Firearms Dashboard – were granted the ability to configure security settings at the workbook level. This was also true at the sheet level, in essence, leaving responsibility with Research Center personnel to properly configure settings to prohibit public access to an underlying dataset. This administrator-level configuration – whereby Data Analyst-1 had the ability to configure Tableau settings at the workbook and sheet

[35] A Tableau administrator account controls the type of access a DOJ personnel has when using Tableau, including the ability to configure security settings at the project level. The Tableau administrator also has the ability to choose whether to make settings uniform across an entire Tableau project or to allow security settings to be configured by individual users at the workbook or sheet level.

levels for the Firearms Dashboard – was actually a default Tableau setting that the Tableau Team never sought to modify. Indeed, it appears that the ADB personnel who were part of the Tableau Team did not even understand that, with their Tableau administrator rights, they had the ability to maintain control and responsibility over all workbook security settings at the project level. It further appears that the Tableau Team, despite being the administrator, did not take sufficient steps to be better informed regarding Tableau security settings; if the ADB personnel on the Tableau Team had taken such steps, they likely would have learned that maintaining administrator control over security settings at the project level to avoid configuration errors at the workbook and sheet levels is a best practice well-documented in Tableau materials.

b. Firearms Dashboard Structure

In order to create the Firearms Dashboard, as was typical of Research Center personnel when creating an OpenJustice dashboard, Data Analyst-1 used an assigned user account to access Tableau Desktop. To do so, Data Analyst-1 created a workbook by uploading the underlying dataset (which included confidential personal data). Within this workbook file, Data Analyst-1 conducted analysis to organize and segregate data from the underlying dataset intended for public viewing into Tableau sheets. Within these sheets, Data Analyst-1 further organized the data into user-friendly visualizations, which was, in essence, a draft of the Firearms Dashboard.

Once this process was complete, Data Analyst-1 published the draft of the Firearms Dashboard to the Tableau staging environment, where Data Analyst-1 was able to further review the data that was intended to be publicly available, as well as test the functionality, appearance, and usability of the Firearms Dashboard. As previously explained above, links to the draft Firearms Dashboard in the Tableau staging environment also were provided to other Research Center personnel, BOF personnel, and ultimately other DOJ personnel and executives, so that they too could review the Firearms Dashboard while still in draft form and make suggested revisions before it was finalized for publication. Once this internal review was finalized, and the required formal DOJ approvals were obtained, a final version of the Firearms Dashboard was uploaded with assistance from ADB personnel to the Tableau production environment for publication on OpenJustice, where it was accessible for public viewing.[36]

When publishing the Firearms Dashboard to OpenJustice, Data Analyst-1 intended to prohibit public viewing or download of the underlying data. Data Analyst-1 configured the Tableau security settings on the Firearms Dashboard at the workbook level in a manner that Data Analyst-1 believed would prevent data download functionality (discussed in further detail below). This was consistent with the step-by-step instructions in an informal written process document that had been created by former Research Center personnel in connection with different OpenJustice dashboards regarding how to upload and publish data to the Tableau production environment and passed on to Data Analyst-1 and other current Research Center personnel. This process document, however, does not reference the need to *also* configure security settings at the *sheet* level in addition to the workbook level. As such, Data Analyst-1 was unaware of the ability or need to configure sheet-level security settings in Tableau and therefore set only workbook-level security settings to restrict public access to the underlying

[36] The Research Center used only one project folder, titled "Default," for all dashboards. This project folder was a default folder existing within Tableau Desktop when the Research Center first started using the software in 2019.

dataset. As a result, sheet-level security settings were left alone and not configured to deny public access to the underlying dataset, which, unbeknownst to Data Analyst-1, rendered as ineffective the workbook-level settings Data Analyst-1 had configured. This failure to configure the sheet-level security settings resulted in the public's ability to access the underlying dataset containing confidential personal data.

c. Data View and Download Functions

Generally, it was not unusual for public visitors to OpenJustice to be able to view or download certain information. In fact, a section of the OpenJustice website (separate from interactive Tableau dashboards) has resources and data available in .pdf and .csv files. DOJ personnel generally understood, however, that the only data available on OpenJustice was aggregated, anonymized data that was appropriate for public viewing and download. Therefore, it would not necessarily have been of particular concern for a reviewer of the Firearms Dashboard to see some sort of feature to download data enabled on the Firearms Dashboard. Nonetheless, no DOJ reviewers inquired about or sought further information about what download capabilities (if any) were available to public visitors to the Firearms Dashboard. If a reviewer had observed and inquired about data download functionality that was in fact active (because of a failure to set the Tableau security settings correctly), the inquiry may have revealed that the underlying dataset (and the confidential information contained therein) was publicly accessible.

As discussed above, where the intent is to prohibit public access to the underlying dataset for viewing or download, either: (1) the Tableau administrator should restrict the project-level security settings to deny public view and download such that the project-level permissions cascade to the workbook or sheet level (regardless of whether any DOJ personnel without administrator authority using Tableau configures the workbook or sheet security settings to permit public users to view or download the underlying dataset); or (2) the DOJ personnel conducting analyses on Tableau should restrict the security settings at both the workbook and the sheet levels to deny the public access to the underlying dataset. Unfortunately, neither configuration occurred here.

The investigation found that there were two ways the underlying dataset for the Firearms Dashboard could be viewed and/or downloaded by the public: (1) the Toolbar's "Data" option; and (2) the Tooltip hover feature's "View Data" option. It was not possible to accurately determine which feature was used by public visitors to download confidential personal data from the Firearms Dashboard on OpenJustice from June 27-28.

Toolbar "Data" Download Option

By default, a "Toolbar" appears either at the top or bottom of the dashboard. One of the options on the Toolbar is "Download" (*Figure 1 at arrow*).[37]

[37] All images (described as figures) in this Report are representative screen images that are not intended to reflect actual data posted on OpenJustice.

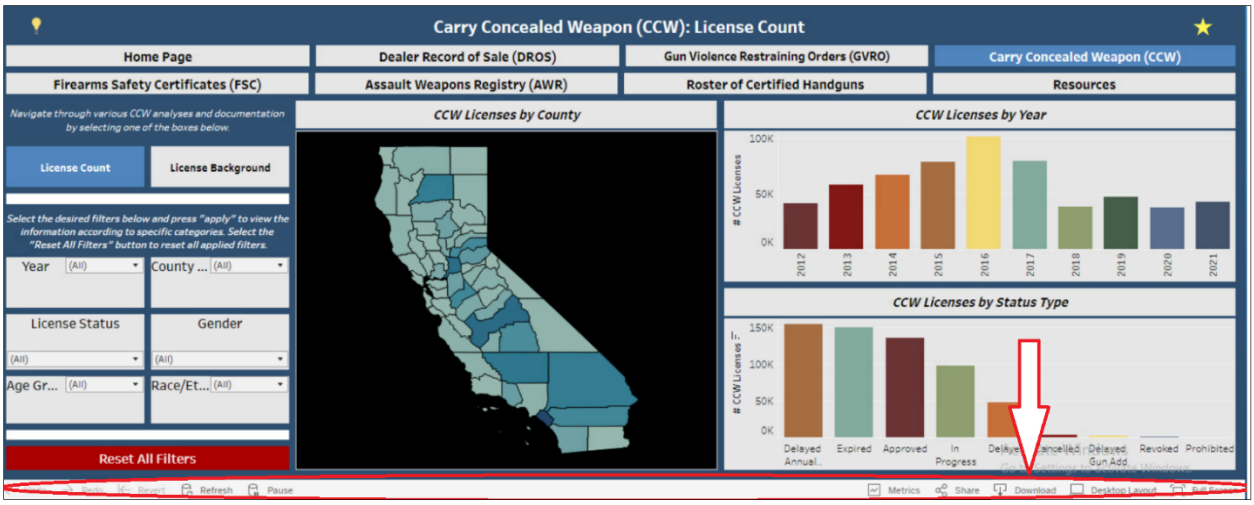


Figure 1

When "Download" is selected, a dialog box opens with an additional option to download "Data." If no visualizations are selected on the dashboard, or security settings are configured to restrict the ability to download data, the "Data" option will be greyed out, *i.e.*, the feature is inactive (*Figure 2 at oval*).

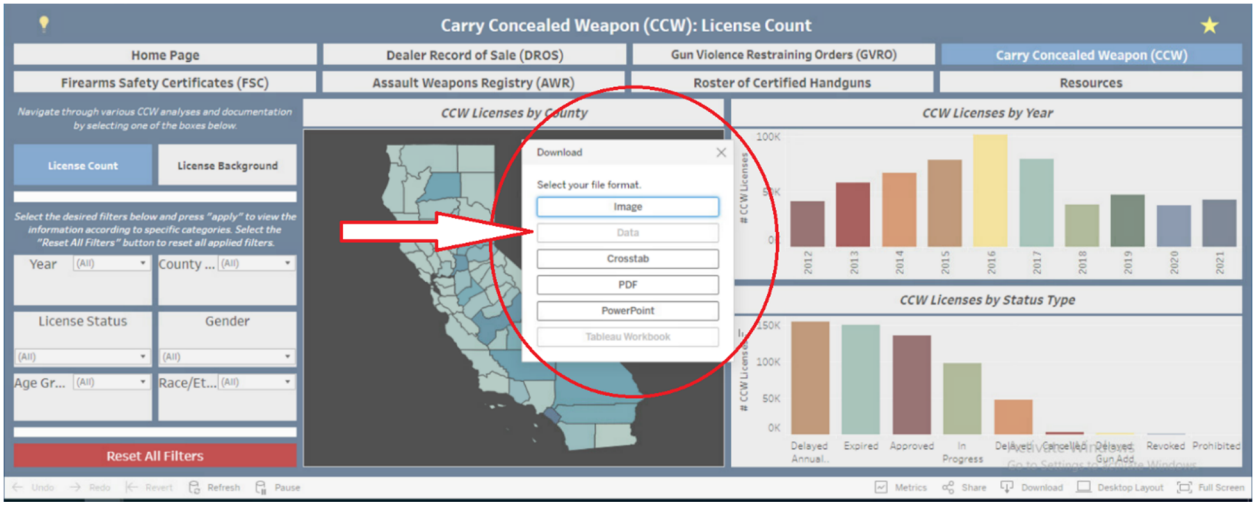


Figure 2

But, regardless of how security settings are configured at the workbook level, if the security settings at the *sheet* level are configured to allow the ability to download data, as set for the Firearms Dashboard (unbeknownst to Data Analyst-1 or apparently anyone else at DOJ), *and* a visualization feature from the Firearms Dashboard is selected (for example, as shown below, if a county on the displayed map of California is selected), the "Data" option will appear black and be functional (*Figure 3 at oval*).

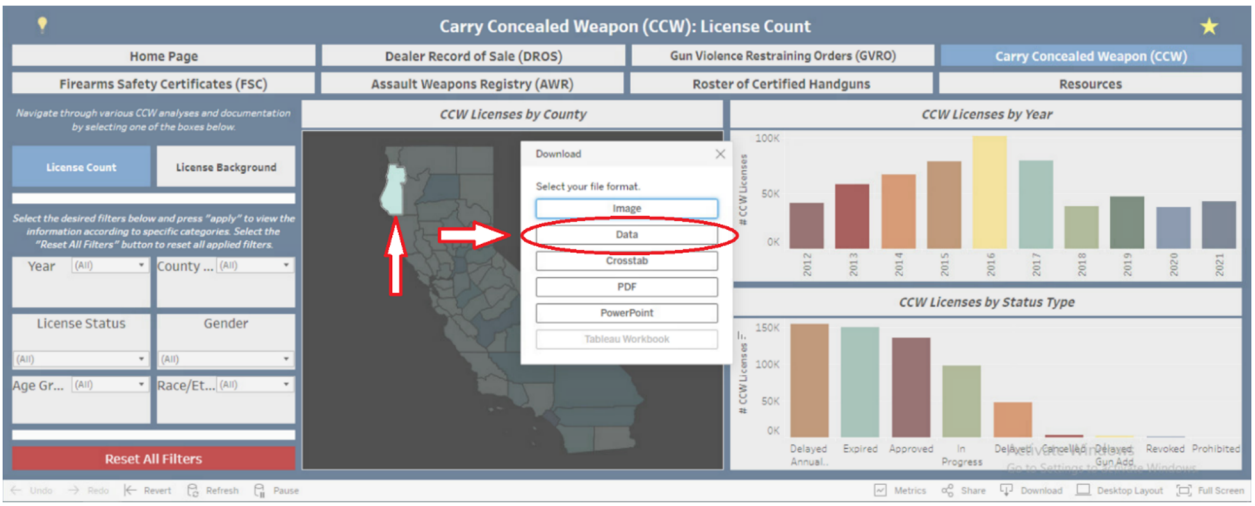


Figure 3

In this scenario, selecting the "Data" option provides access to the underlying dataset, as displayed below (*Figure 4*), which allows a public visitor to toggle between viewing and downloading summary data or the full underlying dataset. Summary data contains the fields used to generate the visualization, while the full underlying dataset contains all the fields Data Analyst-1 uploaded into Tableau to create the workbook (whether or not a field was used in the dashboard visualization).

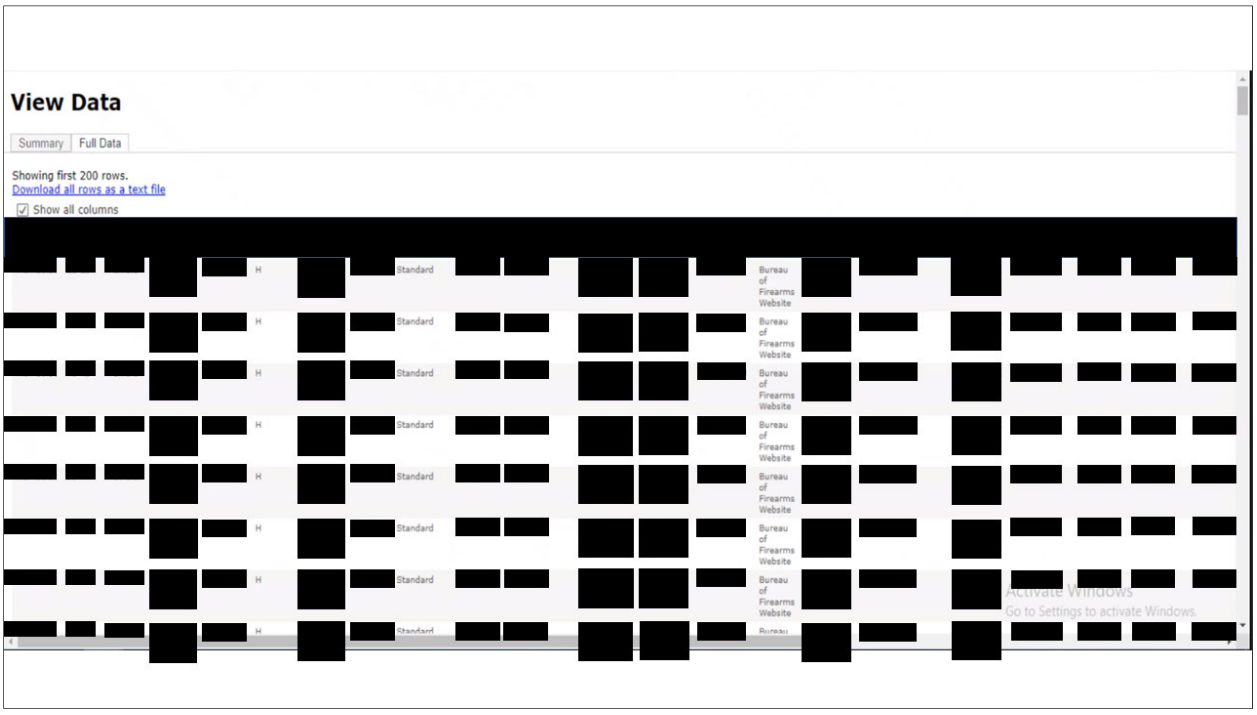


Figure 4 (confidential personal data has been redacted)

Therefore, despite the security settings configured by Data Analyst-1 at the *workbook* level, because of how the security settings were set at the *sheet* level – again unbeknownst to Data Analyst-1 or apparently anyone else at DOJ – the underlying dataset was in fact publicly

accessible for viewing and download through the Toolbar "data" download option when the Firearms Dashboard was published.

Tooltip Hover Feature's "View Data" Download Option

In addition, the Tooltip is an optional feature, *i.e.*, not a default setting like the Toolbar, in Tableau that provides additional functionality to a public visitor when hovering over a dashboard visualization with a mouse. This functionality allows a public visitor to select a "View Data" option which, when selected, allows the visitor to view the underlying dataset. The screenshot (*Figure 5*) below shows the mouse hovering over a particular county on the visualization of the map of California, causing the Tooltip to appear in a new dialog box.

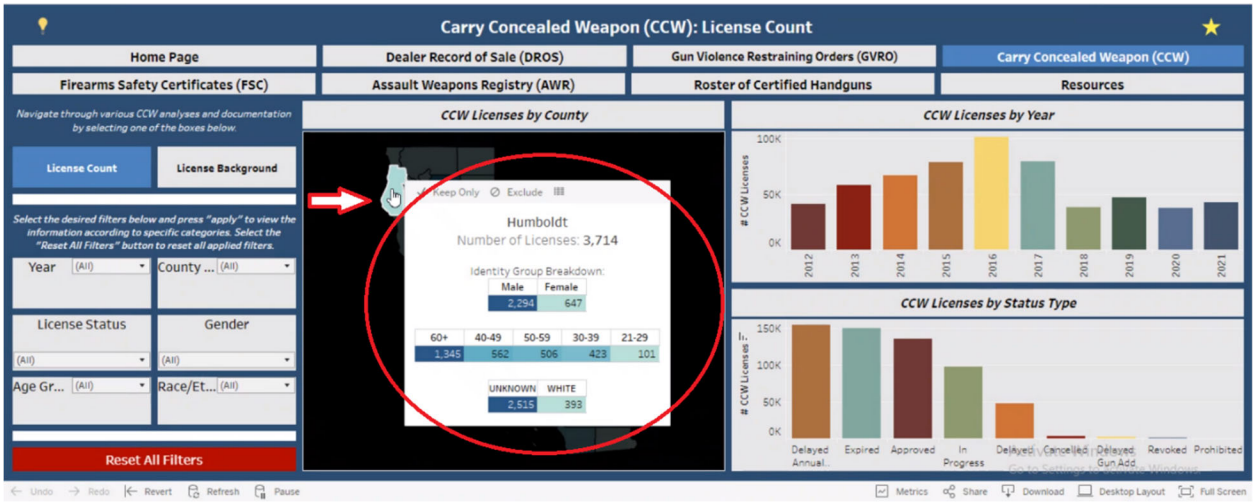


Figure 5

Within the dialog box, if a public visitor then hovers the mouse over a three bar icon at the top of the dialog box, an option to "View Data" will appear (*Figure 6*).

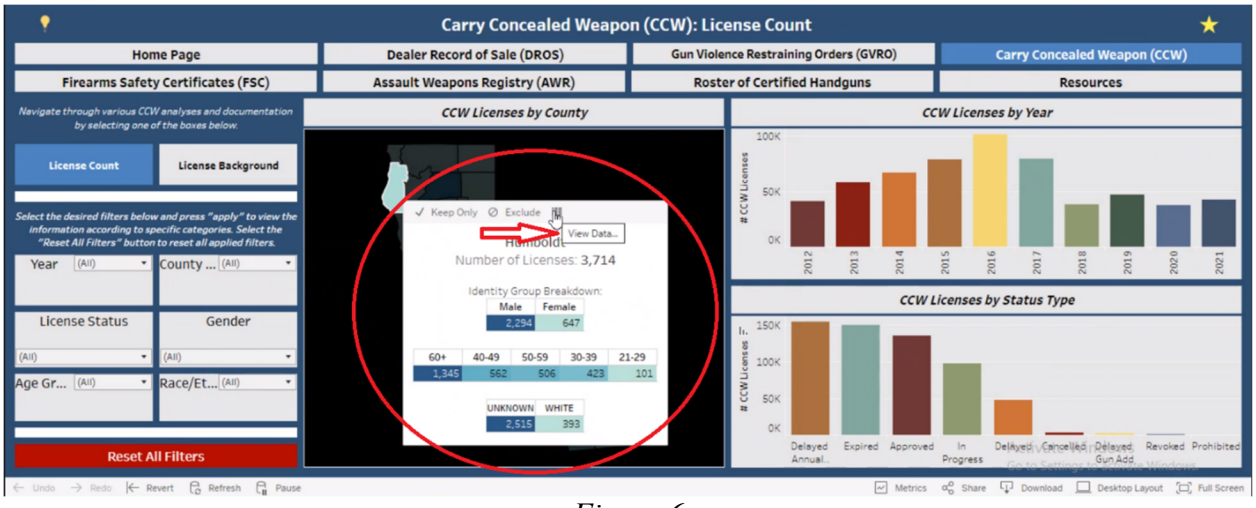


Figure 6

If security settings allow, the public visitor can then select "View Data" and is presented with an option to view either a summary or the full underlying dataset and to download it, as shown below (*Figures 7 and 8*).

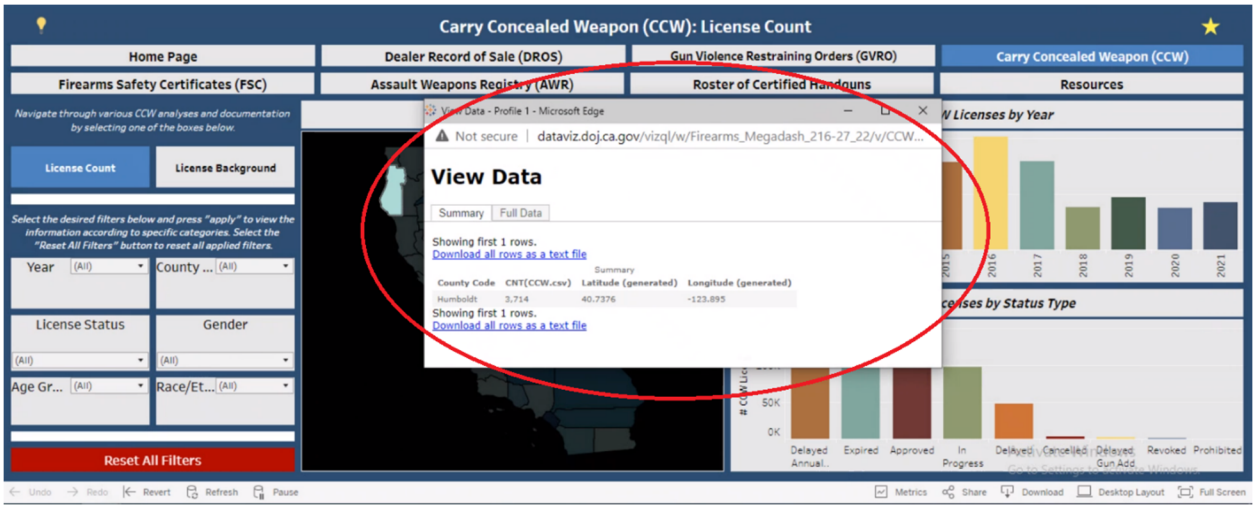


Figure 7

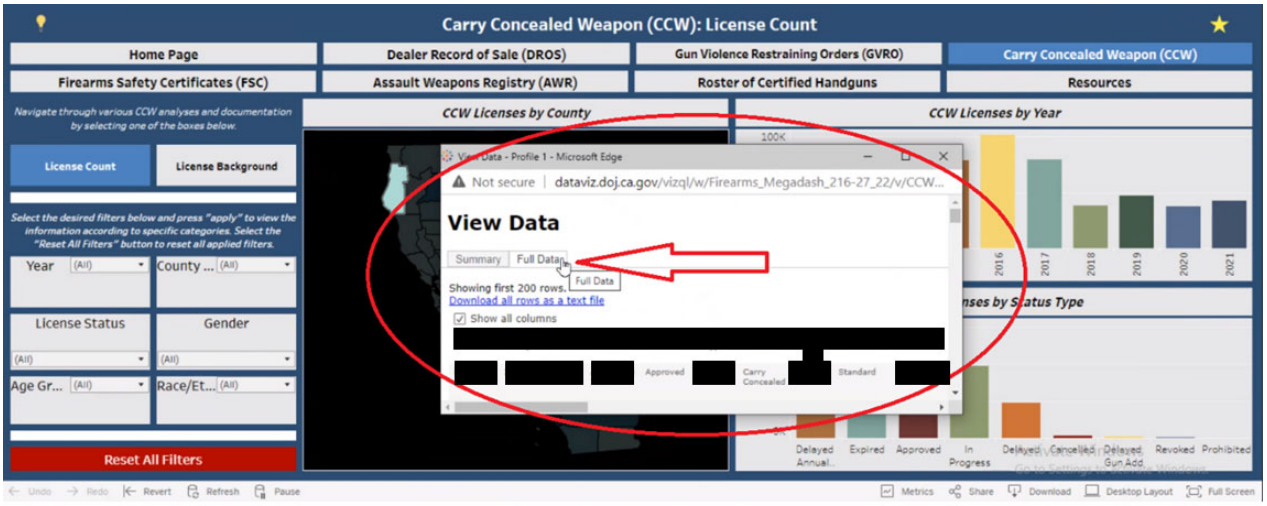


Figure 8

The image below displays what the public visitor would see if they select "Full Data" (*Figure 9*).

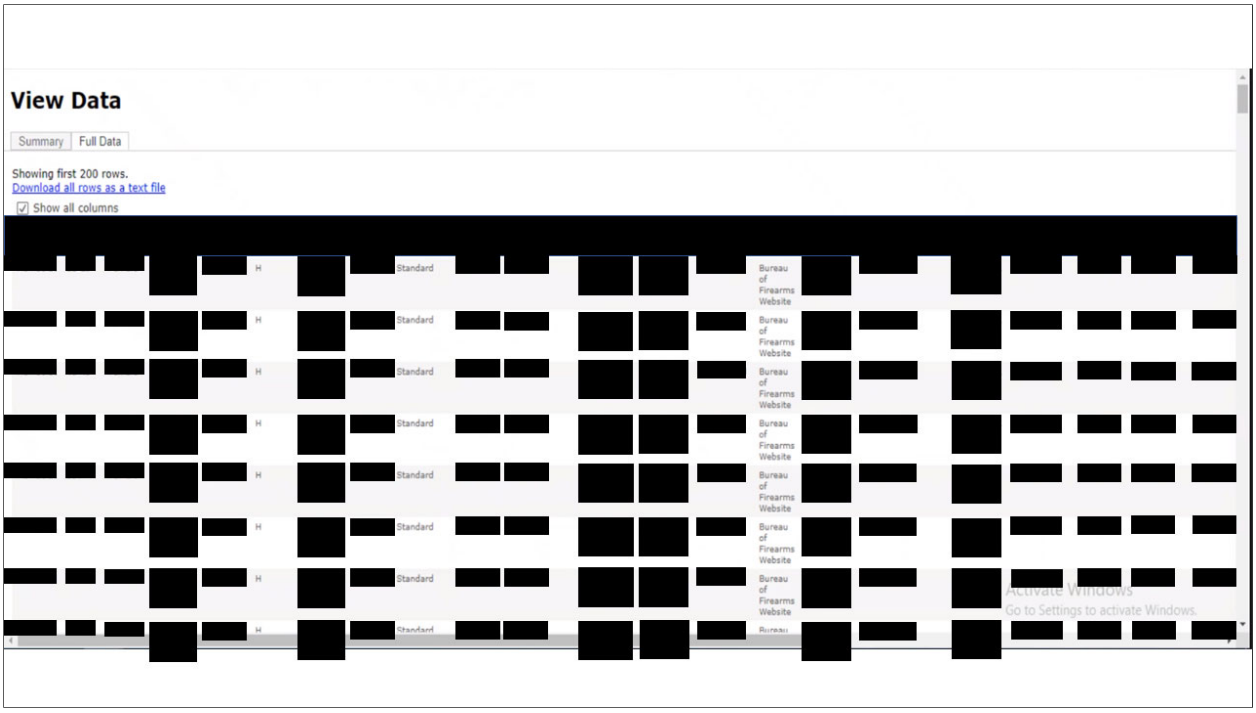


Figure 9 (confidential personal data has been redacted)

Data Analyst-1 was aware of the Tooltip option but believed its functionality was disabled because of how Data Analyst-1 had set Tableau security settings at the *workbook* level. But because the security settings were not also configured at the *sheet* level to preclude public access to the underlying dataset – again unbeknownst to Data Analyst-1 or apparently anyone else at DOJ – this feature allowing public access to the underlying dataset with confidential personal data was in fact active when the Firearms Dashboard was published.

* * *

As described and displayed above, the Tableau Team, as administrators of Tableau, failed to better understand and exercise their administrator rights to manage security settings at the project level to avoid misconfiguration at the workbook and sheet levels. The Tableau Team also failed to confirm that Data Analyst-1 had an appropriate understanding of how the security settings could and should be configured.

Further, lacking awareness of administrator rights and project-level settings, Data Analyst-1 believed that the security settings were properly configured to preclude public access to the underlying dataset. As a result, Data Analyst-1 – in reliance solely on the informal process document passed on from former Research Center personnel regarding how to publish Tableau dashboards – failed to configure security settings at both the workbook and sheet levels to preclude public access to the underlying dataset. Data Analyst-1 also did not seek, nor was directed to do so by a supervisor, input or assistance from the Tableau Team or Tableau technical support to verify that security settings for the Firearms Dashboard were properly configured.

D. DOJ Discovery of June 27-28 Data Exposure

Key Findings:

- After receiving a direct message via social media on June 27 stating that confidential personal data was accessible to the public on the Firearms Dashboard, the Attorney General promptly asked the CDAG to determine whether the claim was true.
- While probing the validity of the claim that confidential personal data was accessible to the public on the Firearms Dashboard, CJIS personnel learned that: (1) the Tableau server was down but did not connect that fact to potential exposure and download of confidential personal data; and (2) confidential personal data had been uploaded unnecessarily by Data Analyst-1 to the Tableau server as part of the underlying dataset even though it was not intended to be visible to the public.
- Based on repeated assurances by the Research Center Director (based on discussions with Data Analyst-1) that confidential personal data could not be accessed by the public, the CJIS Chief assured the CDAG of the same; the CJIS Chief, however, never informed the CDAG that confidential personal data had been unnecessarily included in the underlying dataset.
- Without conducting further investigation or consulting with the CDAG, the CJIS Chief directed that the Firearms Dashboard with the underlying dataset containing confidential personal data should go live again after the Tableau server was restored the night of June 27.
- Although DOJ personnel promptly investigated the report of a possible data exposure, these efforts were undermined by lack of effective coordination and communication between various CJIS components, an overall lack of technical expertise, and the failure of DOJ personnel, including certain supervisors, to more closely probe the cause of the server outage and to verify assertions by Data Analyst-1 that confidential personal data was not publicly accessible.
- It was not discovered that the public could view the underlying confidential personal data until the morning of June 28; DOJ personnel's prior assurances to the contrary were based on an incomplete review of the Firearms Dashboard active functionality and an erroneous understanding of Tableau security settings.

1. DOJ Alerted of Potential Exposure of Confidential Personal Data

At 6:15 p.m. on June 27, 2022, a user unknown to the Attorney General sent direct messages to the Attorney General's personal Twitter account stating that the Firearms Dashboard made confidential personal data available to the public, including addresses and dates of birth for CCW permit holders. These messages included attached media (later learned to be two screenshots of the Firearms Dashboard as public visitors likely would have seen it that evening). The attached media was hidden and could not be viewed without selecting an option to "view media."[38]

[38] The Attorney General uses two Twitter accounts: one in his official capacity as the Attorney General, another in his personal capacity. Members of the Attorney General's campaign staff have access to his personal Twitter account, but their access is generally for the purpose of posting public-facing campaign content, not for retrieving or checking direct messages sent to the Attorney General, which he typically handles himself, as he did on the evening of June 27.

Consistent with the Attorney General's typical practice when receiving messages and attachments via social media from unknown senders, to avoid phishing scams or other malicious efforts, the Attorney General did not respond to the messages or open the media.[39] Rather, the Attorney General promptly took screenshots of the direct messages and sent them via text message to the CDAG and his Chief of Staff, directing them to determine if confidential personal data was in fact publicly accessible on the Firearms Dashboard. In that same text message, the Attorney General also emphasized that personal identifying information that is protected under the law should not be disclosed.

Immediately upon receiving the messages from the Attorney General, at 6:30 p.m., the CDAG sent text messages to the CJIS Chief, requesting a call as soon as possible because someone had sent the Attorney General a message that confidential personal data was available on the Firearms Dashboard for CCW permit holders. Immediately thereafter, the CJIS Chief called the Research Center Director and explained that confidential personal data may be publicly accessible on the Firearms Dashboard. The CJIS Chief then informed the CDAG that the matter was under review.

The CJIS Chief's initial view was that the messages to the Attorney General were likely a hoax since DOJ had previously received false reports and claims regarding other matters. The CJIS Chief did not ask to see the original messages received by the Attorney General. Further, because the CJIS Chief understood and believed that OpenJustice dashboards only displayed aggregated, non-confidential data, security concerns regarding OpenJustice had always been a low priority and not a focus for the CJIS Chief. As such, while the report was being taken seriously, the CJIS Chief was not overly concerned at the time that confidential personal data was publicly accessible.

2. DOJ Review of the Firearms Dashboard Upon Notification

Immediately after being notified by the CJIS Chief on the evening of June 27, the Research Center Director attempted to access the Firearms Dashboard on OpenJustice but was unable to do so because the Tableau server was apparently down and instead received an error message as shown below (*Figure 10*).

[39] During this investigation, copies of these direct messages were retrieved at the direction of Morrison Foerster, at which time the attached media was viewed for the first time, revealing the screenshots.

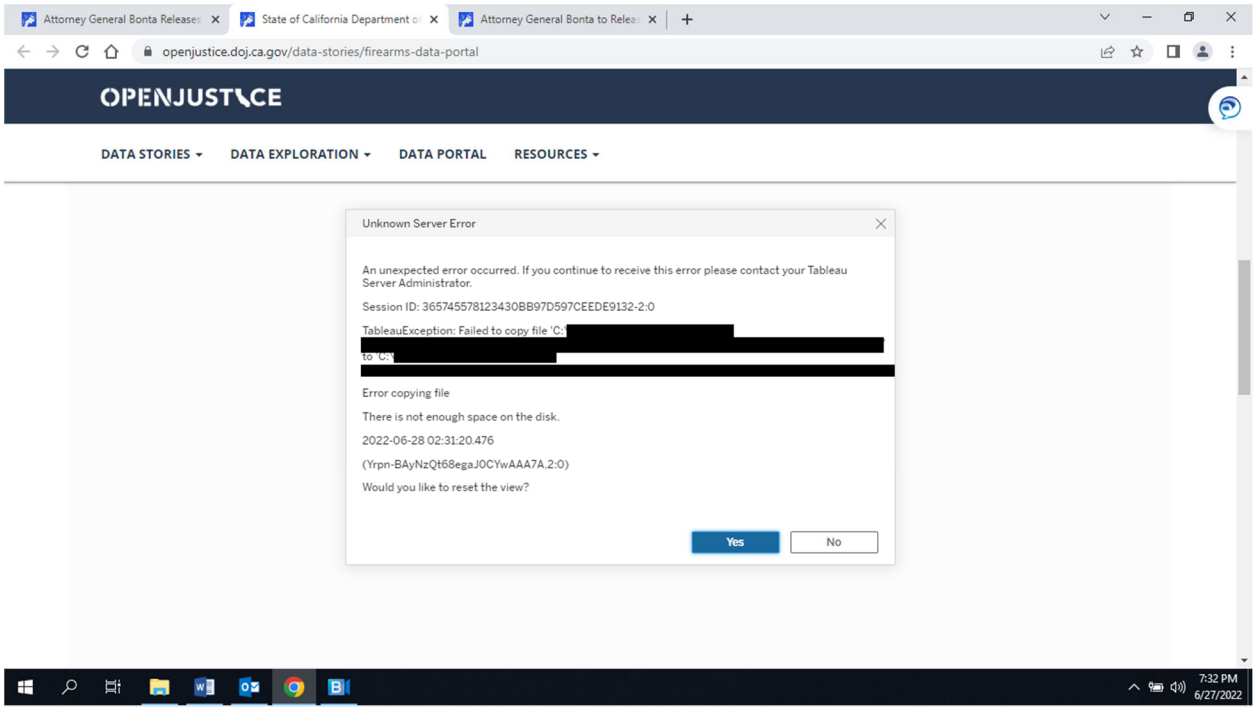


Figure 10 (file path redacted)

Around that same time, the Research Center Director attempted to call Data Analyst-1's direct supervisor, but the supervisor was unavailable. The Research Center Director then called Data Analyst-1 and shared the claim that confidential personal data was available to the public on the Firearms Dashboard but that the Tableau server appeared to be down. Data Analyst-1 then attempted to access OpenJustice but also was unable to do so. The Research Center Director then informed the CJIS Chief that the Tableau server was down and, as a result, the public could not access the Firearms Dashboard and Research Center personnel could not view it to assess whether confidential personal data was accessible on it.

The CJIS Chief then became concerned that perhaps there had been a hack affecting the server. Accordingly, the CJIS Chief called and informed the ADB Director that, in seeking to look into a claim that confidential personal data was publicly accessible on the Firearms Dashboard, the Research Center had learned that the Tableau server appeared to be down; thus the Firearms Dashboard (as well as other dashboards) could not be accessed and viewed. The ADB Director directed ADB personnel to investigate the status of the server (but not the claim regarding confidential personnel information being available). ADB personnel confirmed that, while OpenJustice was still operational and accessible, the Tableau server hosting the Firearms Dashboard (and other dashboards) was down so that the dashboards were not viewable on OpenJustice. ADB personnel continued to investigate the issue and, at 7:30 p.m., determined that the Tableau server hosting the Firearms Dashboard was down because the server appeared to have run out of storage space.

At the same time ADB personnel sought to address the Tableau server issue, Research Center personnel continued to assess whether confidential personal data had been made publicly accessible on the Firearms Dashboard. Because the public-facing Firearms Dashboard in the

Tableau production environment was not available while the Tableau server was down, the Research Center Director and Data Analyst-1 – who were communicating via a continuing video conference – accessed and viewed the Firearms Dashboard in the Tableau staging environment (*i.e.*, where the draft Firearms Dashboard had been internally reviewed before it was published). As they conducted this review, Data Analyst-1 asserted that there was no ability for the public to view or download the underlying dataset from OpenJustice. As has since been determined, however, this review apparently did not include reviewing all of the functionalities available to public visitors to the Firearms Dashboard or recognizing that there were active Toolbar and Tooltip features that enabled public access to the underlying dataset when the Firearms Dashboard was live on OpenJustice. Data Analyst-1 also showed the Research Center Director how the workbook-level Tableau security settings had been configured, believing at the time that such settings precluded public access to the underlying dataset.

Seeking to assess further whether confidential personal data could have been accessed by the public, the Research Center Director also directed Data Analyst-1 to review the underlying dataset uploaded to the Tableau server. According to the Research Center Director, Data Analyst-1 gave assurances that there was no confidential personal data in the underlying dataset. When the Research Center Director reviewed the dataset while on the video conference with Data Analyst-1, however, the Research Center Director saw that there was confidential personal data (including full names and residential street addresses) associated with CCW permit holders in the underlying dataset. The Research Center Director was shocked, believing there was no purpose for this confidential personal data to have been included by Data Analyst-1 in the underlying dataset. According to the Research Center Director, Data Analyst-1's unnecessary inclusion of this data was inconsistent with Research Center protocols for uploading and handling data, both because excess data uses up limited server storage space and because sensitive data should only be used as necessary, *i.e.,* "need-to-know, right-to-know." The Research Center Director recalled that Data Analyst-1 also appeared shocked by this revelation and at no point indicated that the upload of the underlying dataset with this confidential personal data had been intentional.

Data Analyst-1's account differed. Data Analyst-1 did not recall telling the Research Center Director that there was no confidential personal data in the underlying dataset or expressing any surprise during the video conference. Data Analyst-1 claimed to have always known and intended to include confidential personal data in the underlying dataset for perceived efficiencies (as detailed in Sections VI.B.2 and VI.B.3 above). Data Analyst-1 further claimed that if the Research Center Director perceived Data Analyst-1 to be surprised, it was merely because, at that moment, Data Analyst-1 may have forgotten that there was confidential personal data in the underlying dataset. There is no written or other record of these conversations.[40]

After determining that there was confidential personal data in the underlying dataset associated with CCW-related data, the Research Center Director directed Data Analyst-1 to create a *new* dataset that *excluded* all such data to replace the existing dataset. Data Analyst-1 indicated that a new dataset could be created and ready for upload that evening.

[40] It is unclear whose version of events is accurate; regardless, by the evening of June 27, both the Research Center Director and Data Analyst-1 were aware that confidential personal data was included in the underlying dataset.

That same night, at 7:00 p.m., the Research Center Director informed the CJIS Chief, who was also surprised to learn, that there was confidential personal data in the underlying dataset uploaded to Tableau for the Firearms Dashboard. The Research Center Director also reported, however, that Data Analyst-1 and the Research Center Director had reviewed the Firearms Dashboard in the staging area and were unable to replicate any way the public could access the underlying dataset. The Research Center Director further reported to the CJIS Chief that Data Analyst-1 had displayed for the Research Center Director the Tableau security settings that Data Analyst-1 claimed precluded public access, along with repeated assurances that there was no way for the public to access the underlying dataset. Based on this information, the Research Center Director and CJIS Chief believed that confidential personal data had not been publicly accessible and would not be accessible once the server issue was resolved and the Firearms Dashboard went live again (although they were unable to further confirm this on the public-facing Firearms Dashboard because the Tableau production environment was still down). Around 7:15 p.m., the CJIS Chief spoke with the CDAG via telephone and conveyed that confidential personal data was not publicly accessible, but did not share that there was confidential personal data in the underlying dataset.

At some point during the evening of June 27 (while the Research Center Director and Data Analyst-1 continued to assess whether confidential personal data was publicly accessible on the Firearms Dashboard), Data Analyst-1 and the Research Center Director learned that, in addition to the initial message received by the Attorney General, a few comments making similar claims had been posted by unknown users on OpenJustice (which has a public comment feature). The CJIS Chief recalled hearing that night (but did not recall from whom) about a comment posted on OpenJustice that "PID" was publicly available. In the CJIS Chief's view, however, because the comment used what the CJIS Chief perceived as a typo or incorrect terminology ("PID" instead of "PII"),[41] the report did not appear credible (and was likely from the same individual who made the initial report to the Attorney General because that individual also had used the term "PID," which was unfamiliar to the CJIS Chief). The CJIS Chief therefore continued to believe the report was a hoax.

Sometime later that evening, the Research Center Director explained to the CJIS Chief that Data Analyst-1 had been directed to create a new underlying dataset with CCW-related data that did not include confidential personal data and it would be ready for uploading that same evening once the Tableau server issue was resolved. Although the Research Center Director preferred to replace the underlying dataset before the Firearms Dashboard went back online, it was late in the night and replacing the underlying dataset could impact the visualizations on Tableau and replacing a dataset late at night also could lead to inadvertent mistakes. Ultimately, it was the CJIS Chief's call to make and, given the late hour and based on the assurances provided that confidential personal data was not publicly accessible, the CJIS Chief decided, without consulting the CDAG, that replacing the underlying dataset could wait until the next morning even if the Tableau server was restored and the Firearms Dashboard went live again that night.

At 10:00 p.m., via text, the CJIS Chief reported back to the CDAG for the first time since 7:15 p.m. While the CJIS Chief informed the CDAG that a claim that confidential personal data was available also had been posted in a comment on OpenJustice, the CJIS Chief assured the CDAG

[41] PID, however, can be understood to refer to "personal identifiable data."

that everything had been "triple checked" and no confidential personal data was publicly accessible on the Firearms Dashboard. The CJIS Chief also stressed to the CDAG that any publicly accessible data on OpenJustice was "strictly statistical in nature." Relying on these representations, the CDAG reported to the Attorney General that confidential personal data was not publicly accessible. As noted above, however, the CJIS Chief failed to report to the CDAG the revelation that there was confidential personal data in the underlying dataset or that the CJIS Chief had decided that the underlying dataset did not need to be replaced until the next morning even if the Tableau server was restored and the Firearms Dashboard (with the underlying dataset containing confidential personal data) went live again that night.

At the same time that Research Center personnel were probing whether confidential personal data was accessible to the public, ADB personnel, as well as TSB personnel[42] who had been called in to assist, continued to seek to resolve the server issue. They were only focused, however, on getting the Firearms Dashboard operational, not on whether confidential personal data was accessible by the public.

As part of their efforts, ADB personnel, with the support of some TSB personnel, met with Tableau representatives via video conference to troubleshoot the server outage. It was discovered that night that the Tableau server had not been configured by ADB according to best practices when first deployed because it was stored on a drive with limited storage space, which was believed to have contributed to the server being down. ADB personnel have since acknowledged that the number of public visitors to the Firearms Dashboard alone could not have overloaded a server with the storage capacity that then was available. ADB personnel also acknowledged that they did not attempt to further investigate the root cause of the outage and why the Tableau server appeared to have run out of space or investigate whether the outage was connected in any way to the claim that confidential personal data might be publicly accessible on the Firearms Dashboard. Indeed, there was not uniform knowledge across all ADB personnel involved in reviewing the Tableau server issue of this claim, with some ADB personnel having no recollection of having been informed of it. And, to the extent there was knowledge of the claim that night, little if any attention was paid to it by ADB personnel in relation to their efforts to resolve the server outage.

ADB and TSB personnel instead focused only on server size expansion, including reviewing event logs for error messages and audits of messages, but did not see anything that they believed was unusual. One TSB employee observed an error message that suggested there was not enough space on the server due to temporary files being created by public site visitors downloading data. This TSB employee, however, did not recall being informed of the claim that confidential personal data was publicly accessible and therefore did not appreciate the potential significance of this error message in relation to this claim.

The investigation has since determined that the outage was caused by the creation of temporary files using up space on the Tableau server as a result of public visitors seeking to download the underlying dataset with confidential personal data. A screenshot of this error message is provided below (*Figure 11*).

[42] As discussed above, TSB personnel responsible for server infrastructure and software used to support DOJ operate in a 24-hour computing environment to ensure all systems are available.

Figure 11 (file path redacted)

The Tableau server came back online around 9:30 p.m. the evening of June 27, with the original underlying dataset containing confidential personal data still uploaded to the Firearms Dashboard and again accessible to the public. After the Tableau server came back online, around 10:00 p.m., the Research Center Director and Data Analyst-1 also reviewed the public-facing Firearms Dashboard. In this review, they did not see confidential personal data and failed to identify any way for the public to access the underlying dataset or the confidential personal data in the underlying dataset. Again, however, this review apparently did not include reviewing all of the functionalities available to public visitors to the Firearms Dashboard (such as the active Toolbar and Tooltip features described above).

Throughout the evening of June 27 into the early morning of June 28, it does not appear that Research Center, ADB, or TSB personnel coordinated or communicated effectively regarding the multiple issues they were trying to resolve. While Research Center personnel were focused on investigating whether confidential personal data was publicly available, ADB and TSB personnel were focused on getting the Tableau server back online. There also was a general sense of pressure perceived by the DOJ personnel involved in these efforts to get the Firearms Dashboard back online because its launch had occurred earlier that day and been publicly announced; they were concerned that it would not reflect well on DOJ if the Firearms Dashboard went down that same day. Consistent with this concern, the CJIS Chief expressed the belief that operational readiness is important to CJIS's reputation. There thus was a sense of urgency felt by some CJIS personnel that evening to make the Firearms Dashboard operational again as quickly as possible. There is no evidence, however, of an explicit directive or pressure from other DOJ executives to restore the Firearms Dashboard that night.

Early the next day on June 28, at 6:30 a.m., Data Analyst-1 uploaded a revised underlying dataset without confidential personal data associated with the CCW-related data. Confidential personal data associated with FSC, DROS, and AWR-related data (which had not yet been

detected by DOJ as being publicly accessible), however, remained publicly accessible until the Firearms Dashboard was taken offline later that morning at 11:45 a.m., as discussed further below.

3. Confirmation of Data Exposure and Firearms Dashboard Taken Down

On the morning of June 28, the public-facing Firearms Dashboard was available to the public online. Following the events of the prior day and to further assess whether the issues had been fully resolved, the Research Center Director directed Data Analyst-1 to check the OpenJustice website comments. Data Analyst-1 found multiple additional comments claiming that confidential personal data had still been publicly accessible *after* the Tableau server issue had been resolved and the Firearms Dashboard went live again.[43] The Research Center Director immediately sought assistance from the ADB Director to further probe the Firearms Dashboard. Between 8:00 and 9:00 a.m., the ADB Director reviewed the Firearms Dashboard as any member of the public would, and the ADB Director discovered an active "View Data" function within a hover window that enabled public visitors to view and download the underlying data.[44]

At that time, because Data Analyst-1 had already replaced CCW-related data in the underlying dataset, it was believed that confidential personal data was no longer publicly accessible, but the implication was clear: confidential personal data had been publicly accessible on the Firearms Dashboard. Further, this investigation later found that, although Data Analyst-1 had removed confidential personal data associated with CCW-related data, there remained confidential personal data associated with FSC, DROS, and AWR-related data that had never been replaced by Data Analyst-1 and, therefore, had been still publicly accessible.

The Research Center Director promptly alerted the CJIS Chief via text that confidential personal data likely had been available the prior evening until the Tableau server went down, and again through the night and early morning after it had been restored, up until the time Data Analyst-1 replaced the underlying dataset. Because the CJIS Chief believed that the underlying dataset had been replaced with one that did not include any confidential personal data, the CJIS Chief did not order that the Firearms Dashboard be taken down immediately. The CJIS Chief sent a text message at 9:15 a.m. to the CDAG, who was not immediately available, asking for a call to discuss the Firearms Dashboard, but not specifically disclosing this new development. Soon thereafter, at or before 10:45 a.m., the CJIS Chief reported via telephone to the CDAG, for the first time, that confidential personal data had in fact been available to public users on the Firearms Dashboard.

Immediately after the call with the CJIS Chief, at 11:00 a.m., the CDAG convened an emergency call with additional DOJ personnel to further assess the likely data disclosure, while at the same time other DOJ personnel were probing whether confidential personal data might be available on other OpenJustice dashboards. At the outset of the call, given the new information and

[43] The prior evening at 8:00 p.m., at the Research Center Director's request, a Research Center employee had checked the Research Center's inbox for any messages potentially related to the claim that confidential personal data had been publicly accessible on the Firearms Dashboard but found no such emails.

[44] While the ADB Director could not recall which function revealed the accessibility of the underlying data, the ADB Director likely discovered the Tooltip feature described above.

uncertainty, the CDAG directed that the Firearms Dashboard be taken offline immediately, which occurred at 11:45 a.m. During the call, the CDAG also alerted the Attorney General via text at 11:45 a.m. that confidential personal data likely had been exposed and that the Firearms Dashboard had been taken offline. Later that same day, because considerable uncertainty remained regarding the nature and scope of the issues, the CDAG directed that the entire OpenJustice site be taken offline, which occurred at 9:00 p.m.

E. Scope of Data Exposed on the Firearms Dashboard

Key Findings:

- The underlying dataset for the Firearms Dashboard that was publicly accessible contained confidential personal data associated with CCW, FSC, DROS, and AWR-related data; confidential personal data was not included in the underlying GVRO-related data and was never part of the Roster of Certified Handguns data.
- Within the underlying dataset for the Firearms Dashboard, only CCW-related data could be used to independently identify individuals (because the fields exposed included associated names); analysis revealed that none of the other data in the underlying dataset contained information that could be used to independently identify individuals. In total, drawing from the CCW-related data, confidential personal data was exposed on the Firearms Dashboard for approximately 192,000 individuals.
- Even though confidential personal data was exposed in the FSC, DROS, and AWR-related data, the risk from such exposure is limited because the data cannot be used to independently identify individuals (because the fields exposed did not have an associated individual name or other identifier). Further, cross-correlation analysis identified only one possible means of enriching the data that presented limited additional risk; other enrichment of the data required unverifiable assumptions.
- Confidential personal data was available for a period of time that was less than 24 hours: from when the Firearms Dashboard first went live on June 27 until the Tableau server was down and, again, after the Tableau server was restored until it was taken offline on June 28.
- The exposed underlying dataset with confidential personal data was viewed by members of the public and downloaded, in full or in part, approximately 2,734 times across 507 unique IP addresses.
- The decision by the CJIS Chief to go live again with the Firearms Dashboard the night of June 27 after the Tableau server was restored proved to be a compounding error. The vast majority of public downloads of confidential personal data occurred during this latter period of time until the Firearms Dashboard was taken down the next morning at the CDAG's direction.

1. Data That Was Publicly Accessible and Cross-Referencing Analysis

The underlying dataset for the Firearms Dashboard that was publicly accessible on June 27-28 contained CCW, FSC, DROS, AWR, GVRO, and Roster of Certified Handguns-related data. The investigation determined that confidential personal data was contained (and exposed) in only the CCW, FSC, DROS, and AWR-related data. Confidential personal data was *not*

exposed for GVRO-related data because such data had been provided to Data Analyst-1 in aggregate form, nor for the Roster of Certified Handguns-related data, which only contained a list of handguns certified for sale with no confidential personal data.[45]

Within the underlying dataset that contained confidential personal data and was exposed on the Firearms Dashboard, *only* the CCW-related data could be used to independently identify individuals. Specifically, the CCW-related data included data for the years 2012 to 2021 and included the following fields: name, date of birth, street address associated with the permit, gender, race, county, CCW License Number, status of CCW applications, and California's Criminal Identification and Information/State Identification number (also referred to as "CII").[46] The CCW-related data contained approximately 192,000 unique CII numbers, which corresponds generally to the number of individuals for whom CCW-related data (including confidential personal data) was exposed.

Analysis determined that *none* of the remaining other three datasets that contained confidential personal data could be used to independently identify individuals. So while the FSC, DROS, and AWR-related data included fields containing confidential personal data, these fields did not have an associated individual name or other identifier. More specifically:

- The FSC-related data covered the years 2015 to 2021 and included approximately more than 2 million driver's license numbers, issue dates, and dates of birth, but did not include sufficient information to independently identify these individuals (such as names).[47]

- The DROS-related data covered the years 2012 to 2021 and contained information on approximately more than 8.7 million gun sale transactions, which included fields of information for individuals involved in such transactions, including date of birth, gender, and county of the sale, as well as weapon details, transaction date and time, transaction type, transaction status, originating agency identifier (or ORI) number (which identifies the law enforcement agency with jurisdiction over the location where the sale takes place), dealer's identification number, dealer's street address(es), license status, and license type. The DROS-related data does not contain sufficient information to independently identify individuals nor does it contain any fields that are uniquely issued and unique to any particular individual.

- The AWR-related data covered the years 2012 to 2021 and included dates of birth, gender, county, weapon type (including make and model), registration type, AWR number, and application status. Although the AWR-related data does not include

[45] No social security numbers or individual financial information was in the underlying dataset, therefore no such data was publicly exposed.
[46] A CII number, which is automatically generated during a fingerprint check and used to identify individuals in recordkeeping, is a unique identifier of a person.
[47] Absent associated names, the exposure of driver's license numbers poses limited risk because the known data sources that offer the ability to use a driver's license number to independently identify an individual are non-public repositories (e.g., those operated by law enforcement agencies and/or for which access must be authorized).

sufficient information to independently identify individuals, it also did expose more than 31,000 unique AWR Numbers.[48]

A cross-referencing analysis was conducted to assess the feasibility of using the available data to enrich the information known about an individual identified in the CCW-related data. To conduct this analysis, FTI used data processing tools to evaluate overlapping fields for correlation among the sets. For example, because the CCW, FSC, DROS, and AWR-related data all contained date of birth information, the analysis sought to determine if any links reliably could be made between the data based on common fields. Through this analysis, FTI was able to identify one possible means of enriching the data, but the results of this enrichment presented only limited additional risk.[49] Other attempts to make correlations among the data necessitated unverifiable assumptions and did not provide enrichment of CCW-related data.

Accordingly, even though confidential personal data was exposed in the FSC, DROS, and AWR-related data, the risk from such exposure is limited.

2. Data Identified as Downloaded

Pursuant to the methodology described in more detail above, FTI conducted an analysis to identify downloads of the underlying dataset that specifically included the full range of fields with confidential personal data, as compared to downloads of summary data (*i.e.*, fields and aggregate data that did not reveal confidential personal data).

Applying this analysis, the underlying dataset that included confidential personal data (associated with CCW, FSC, DROS, and AWR-related data) was downloaded either partially (*e.g.*, a single or partial selection of counties or years on the Firearms Dashboard) or in full (*i.e.*, all years and geographies available on the Firearms Dashboard) approximately 2,734 times across approximately 507 unique IP addresses on June 27-28.

As described above, the CCW-related data was the only data for which individuals could be positively identified from the confidential personal data. This CCW-related data containing confidential personal data was downloaded either in full or partially approximately 1,467 times across approximately 341 unique IP addresses. Approximately 160 of the approximately 1,467 downloads of the CCW-related data were the full or nearly full sets of the underlying dataset, with approximately 152 of these downloads occurring after the server was restored. The majority of the 1,467 CCW-related data downloads – approximately 1,399 – occurred in the evening of June 27 to the early morning of June 28 after the Tableau server had been restored and the Firearms Dashboard was live again. As previously noted, Data Analyst-1 replaced the CCW-related data on June 28 at 6:30 a.m., therefore, confidential personal data associated with the CCW-related data was not available for public download from that point forward.

[48] Because some individuals may have been assigned more than one AWR number, the analysis could not accurately quantify the total number of individuals whose AWR number was exposed but it is most likely fewer than approximately 31,000.

[49] The enrichment is not disclosed in this Report to prevent potential duplication of it.

Ultimately, the decision by the CJIS Chief to go live again with the Firearms Dashboard the night of June 27 after the Tableau server was restored proved to be a compounding error. The vast majority of public downloads of confidential personal data occurred during this latter period of time until the Firearms Dashboard was ordered to be taken down the next morning by the CDAG.

F. Analysis of Additional OpenJustice Dashboards

Key Finding:

- Although confidential personal data was publicly accessible on the Firearms Dashboard, the investigation did not find that confidential personal data was publicly accessible on any other OpenJustice dashboard.

FTI reviewed and analyzed other dashboards that were or may have at some point been published on OpenJustice to assess whether additional confidential personal data was or had been publicly accessible on those dashboards. FTI's review concluded that although underlying datasets for some of these dashboards were publicly accessible, none of them included confidential personal data.

More specifically, with respect to historical firearms data on OpenJustice prior to when the Firearms Dashboard was published, the underlying datasets were limited to data regarding the weapon and the firearms transaction itself (*e.g.*, year and month of sale, dealer identification, gun make and color codes, caliber, serial number, and barrel length), but did not include data fields containing confidential personal data. Therefore, although these underlying datasets may have been historically publicly accessible, no confidential personal data could have been exposed.

Certain of the other dashboards on OpenJustice included disaggregated data, but based on the available information, it was not possible to conclusively determine whether this data was accessible to the public. Regardless, this disaggregated data did not include confidential personal data that could be used to identify an individual person. For example, although RIPA-related dashboards included disaggregated data on race, gender, age, LGBTQ+ status, and disability status, the data did not contain fields that would have allowed for identification of a particular person, such as name or street address.

VII. POST-INCIDENT MONITORING

During the investigation, FTI identified and implemented various monitoring measures to identify potential sharing or misuse of the exposed confidential personal data. Searches on websites including Twitter, Facebook, Reddit, 4chan, and other sites revealed public discussion regarding the data exposure.

From June 27-28 and on subsequent days, some of the confidential personal data obtained from the Firearms Dashboard was shared online but most of the links containing such data were removed or deleted by the time FTI conducted its investigation. For example, CCW-related data containing names, dates of birth, and addresses of approximately 900 individuals was posted on a

specific site on June 28. As of July 25, the post had been viewed 71 times. This post was reported to the site on July 25, and the post was removed.

FTI also conducted dark web searches from July into November 2022 and was unable to locate or identify any other instances in which confidential personal data from the Firearms Dashboard was available.

Based on these searches, there is no evidence of significant or continuing dissemination of the confidential personal data that was publicly accessible on the Firearms Dashboard on June 27-28.

VIII. RECOMMENDATIONS

Based on this investigation's findings, Morrison Foerster has made certain recommendations to help DOJ develop, implement, and employ practices and procedures that will more effectively prevent against future data exposure incidents. This is in addition to steps DOJ already has taken to prevent future unintended public access to underlying datasets on OpenJustice dashboards. Below is a summary of these recommendations.[50]

Recommendation No. 1 – Review and Update Policies and Procedures: DOJ should conduct a thorough review and update of all DOJ policies and procedures regarding the handling of confidential personal data, including for both internal and external data requests, and the supervision of DOJ personnel handling such data. Reinforcing and formalizing policies and supervisory expectations will standardize practices and improve oversight of the preparation and review process for projects that involve confidential personal and other sensitive data.

Recommendation No. 2 – Enhanced Training: DOJ should provide enhanced trainings regarding the handling of confidential personal data as appropriate, taking into account the specific roles and responsibilities of DOJ personnel. Such training will help ensure DOJ personnel have appropriate knowledge and guidance regarding projects involving confidential personal data and safeguards that should be employed when handling such data.

Recommendation No. 3 – Evaluate Security Risk: DOJ should evaluate the security risk for IT solutions (including Tableau) used for projects that involve confidential personal data (such as OpenJustice) and provide formal training of DOJ personnel regarding the use of these solutions. Evaluating risks and enhancing training will mitigate risks and ensure DOJ personnel have information they need to properly use IT solutions in accordance with best practices and understand when to coordinate with other DOJ components and, as appropriate, outside experts.

Recommendation No. 4 - Centralize and Improve Organizational Structure: From an organizational management and governance perspective, DOJ should more effectively and efficiently centralize and enhance oversight and supervision of organization-wide risk management, data security, and related functions. A team of properly trained and experienced specialists with a sufficiently experienced senior executive should be ultimately responsible for

[50] These recommendations may be added to or modified in the future based on new information or other considerations that may arise during their development and implementation.

data security across all DOJ components, with clear divisions of labor and hierarchy of responsibility.

Recommendation No. 5 – Data Incident Action Plan: DOJ should develop a detailed data incident action plan, with clearly delineated protocols, responsibilities (including internal coordination, communication, and approvals), critical item checklists, and other potentially necessary steps, including consultation with outside experts, in response to future reports of the exposure of confidential/sensitive data in order to effectively and expeditiously ascertain credibility, risk(s), remediation, and mitigation.

Recommendation No. 6 – Clearer Roles in Review and Approval Process: DOJ executives and supervisors in all DOJ components should have clearly defined roles in the review and approval process before any project involving confidential personal data can be approved or released publicly, including sufficiently documented, systematic, and rigorous review of any such projects.

IX. APPENDIX – KEY TERMS DEFINED

Term/Phrase	Definition/Description
AB	Assembly Bill
ADB	Application Development Bureau
AFS	Automated Firearms System
AWR	Assault Weapon Registry
BOF	Bureau of Firearms
CARPOS	California Restraining and Protective Order System
CCW	Concealed Carry Weapon
CDAG	Chief Deputy Attorney General
CII	Criminal Identification and Information
CJIS	California Justice Information Services
CURES	Controlled Substance Utilization Review and Evaluation System
Confidential personal data	Data that was never intended to be publicly disclosed in the dataset underlying the Firearms Dashboard, some of which could be used to identify individuals, is referred to herein as "confidential personal data"; this description of "confidential personal data" is not, nor should it be understood as, the legal definition of "Personal Identifiable Information" (PII), as that term is used in other contexts
Database owner	The department or organization that receives, collects, generates, and/or maintains the original underlying criminal justice data
DOJ	The California Department of Justice
DROS	Dealer Record of Sale
ESB	Enterprise Services Bureau
Firearms Dashboard	An interactive dashboard containing firearms-related data published by DOJ on its OpenJustice website
FSC	Firearms Safety Certificate

Term/Phrase	Definition/Description
GVRO	Gun Violence Restraining Order
IT	Information Technology
ITM	Information Technology Manager
MASS	Managed Application Support Systems
OpenJustice	A DOJ website that publishes criminal justice information and data for the public, including through interactive online dashboards that contain charts and other visualizations
ORI	Originating Agency Identifier
PID	Personal Identifiable Data
PII	Personal Identifiable Information
PRA	Public Records Act
RIPA	Racial and Identity Profiling Act
SDCS	Stop Data Collection System
Tableau	A company that creates and licenses commercially available software for data manipulation and visualization applications, including Tableau Desktop and Tableau Server
Tableau dashboard	A consolidated display of Tableau worksheets and related information in a single place
Tableau Desktop	Tableau tool that provides a computing environment that allows data analysts to produce data visualizations in the form of interactive dashboards
Tableau production environment	Tableau Server environment where DOJ personnel can publish finalized dashboards to OpenJustice for public viewing
Tableau Project	A Tableau folder that contains at least one Tableau file
Tableau Server	Tableau tool that provides staging and production environments
Tableau server	DOJ-managed servers running the Tableau software platform
Tableau Sheet	The format in which content is organized in a Tableau workbook
Tableau staging environment	Tableau Server environment where DOJ personnel are able to test and review dashboards

Term/Phrase	Definition/Description
Tableau Workbook	A Tableau file that contains underlying data and the visualizations created from an underlying dataset
TSB	Technology Services Bureau
Underlying dataset	The underlying dataset that Data Analyst created and uploaded to Tableau for the Firearms Dashboard containing CCW, FSC, DROS, AWR, GVRO, and Roster of Certified Handguns-related data