



June 24, 2019

SENT VIA EMAIL

California Department of Justice
California Justice Information Systems
Joe Dominic, Chief

CLETS Advisory Committee
4949 Broadway Room J231
Sacramento, CA 95820
c/o CLETS Administration Section
Maria Cranston, CLETS Executive Secretary
Email: maria.cranston@doj.ca.gov, Joe.Dominic@doj.ca.gov

**RE: Misuse of the California Law Enforcement
Telecommunications System**

Dear Mr. Dominic and Members of the CLETS Advisory Committee:

I write today on behalf of the Electronic Frontier Foundation to thank the California Department of Justice (DOJ) and the CLETS Advisory Committee (CAC) for their significant progress in increasing oversight of law enforcement misuse of sensitive data systems and to also urge you to continue to improve oversight of the network containing Californians' personal information.

Late last week, the Trump administration announced imminent mass immigration raids across the country, including in California.¹ While the president ultimately delayed the enforcement actions, he has stated they may resume in two weeks. As this threat to our communities looms large, DOJ and CAC must protect our data from misuse by U.S. Immigration and Customs Enforcement (ICE).

In addition to this call for urgent action, we also use this opportunity to make recommendations to improve collection and analysis of misuse-related data next year.

* * *

¹ Alvarez, Priscilla; Geneva Sands, and Maria Santana. CNN.com. "ICE set to begin immigration raids in 10 cities on Sunday." June 21, 2019. Online: <https://www.cnn.com/2019/06/21/politics/ice-immigration-raids/index.html>

Over the last four years, the Electronic Frontier Foundation (EFF), an international non-profit based in San Francisco that advocates for privacy and accountability at the intersection of technology and the law, has paid close attention to law enforcement's misuse of the California Law Enforcement Telecommunications System (CLETS). Last year, DOJ issued a new directive clarifying what qualifies as misuse of CLETS and user agencies' obligations for reporting aggregate misuse each year. Staff has also shifted from a passive stance on misuse reporting to a more proactive approach by implementing a rigorous outreach process to ensure agencies are complying with the requirements of the CLETS Policies, Practices and Procedures (PPP). In addition, in February 2019, DOJ added language to the PPP to implement the protections of the California Values Act, which creates the first step to ensuring federal agencies are not using CLETS for immigration enforcement.

These efforts have improved law enforcement's response rate to misuse reports, giving the public a more complete picture of the scope and frequency of CLETS misuse. We appreciate all of the hard work by staff and committee members to make this happen.

While these actions have had a measurable impact on accountability, we respectfully ask that you consider implementing additional changes discussed below that will further protect the personal data of Californians.

1. Federal Immigration Enforcement Agencies' Conflict With CLETS Misuse Policies

A. Sanctions Against ICE Orange County

In April 2018, DOJ issued an information bulletin to all subscribing agencies making clear that "agencies that fail to report misuse annually will be subject to sanctions, up to and including, removal of CLETS service."² It is now June 2019, and the Orange County office of ICE has failed to make these mandated disclosures.

CAC and DOJ must begin the sanction process for this agency. CAC has three options for sanctioning the agency: a) letter of censure, b) suspension of service, and c) removal of CLETS service. Because ICE Orange County received due warning more than a year in advance of the deadline, EFF recommends that CAC initiate suspension of service, followed by removal of CLETS service should ICE Orange County continue to withhold the mandatory disclosures.

B. DOJ Must Review the U.S. Department of Homeland Security and Its Component Agencies' Use of CLETS

² Cal. Dep't of Justice - Cal. Justice Information Servs. Div., "California Law Enforcement Telecommunications Systems (CLETS) - Requirement to Report CLETS Misuse," Apr. 17, 2018, *available at* <https://www.eff.org/document/clets-information-bulletin-april-17-2018>.

Earlier this year, DOJ updated its CLETS policies following the California Values Act going into effect in January 2018. The California Values Act prohibits state and local law enforcement from using agency resources to assist with immigration enforcement in most cases.³ The law specifically contains a provision that prohibits California agencies from providing personal information about an individual to ICE or CBP.⁴ Accordingly, the DOJ updated the PPP to include the following language:

[F]ederal, state or local law enforcement agencies shall not use any non-criminal history information contained within these databases for immigration enforcement purposes. “Immigration enforcement” includes any and all efforts to investigate, enforce, or assist in the investigation or enforcement of any federal civil immigration law, and also includes any and all efforts to investigate, enforce, or assist in the investigation or enforcement of any federal criminal immigration law that penalizes a person’s presence in, entry, or reentry to, or employment in, the United States.⁵

On June 22, 2019, the President stated via Twitter: “At the request of Democrats, I have delayed the Illegal Immigration Removal Process (Deportation) for two weeks to see if the Democrats and Republicans can get together and work out a solution to the Asylum and Loophole problems at the Southern Border. If not, Deportations start!”⁶

Considering this timeline, DOJ should closely monitor each CLETS transaction conducted by ICE, Customs and Border Protection (CBP), and other U.S. Department of Homeland Security (DHS) component agencies. Should DOJ have reason to believe the data is being accessed for immigration enforcement purposes, DOJ should immediately suspend access. While DOJ is required to provide access to criminal history records to these agencies, DOJ can require criminal history requests be filed directly in writing instead of unfettered access through CLETS.

Moreover, DOJ should also audit ICE, CPB, and other DHS component agencies to determine whether they have already misused CLETS. Records provided to EFF through the California Public Records Act showed that not a single entity within DHS reported that it conducted a misuse investigation in 2018. While one may not expect an agency to always issue a positive finding of misuse, it is unusual for an agency the size of DHS and ICE to not open any misuse investigations.

³ S.B. 54, *codified at* Cal. Gov’t Code §§ 7282 *et seq.*

⁴ Cal. Gov’t Code §§ 7284.6(a)(1)(D).

⁵ Cal. Dep’t of Justice - Cal. Justice Information Servs. Div., “California Law Enforcement Telecommunications System Policies, Practices and Procedures,” at 30, Feb. 2019, *available at* <https://www.documentcloud.org/documents/5996502-Clets-Ppp-022019.html>.

⁶ Online: <https://twitter.com/realDonaldTrump/status/1142506687020130306>

In February 2019, the news outlet Voice of San Diego issued a report that ICE officers obtained copies of driver license information in immigration arrests.⁷ All information indicates this access occurred through CLETS. Even if ICE believes its access to CLETS was warranted, it is reasonable at the very least, to expect that an investigation would have been opened.

We are also alarmed by other practices demonstrated by DHS and its component agencies that could pose risks to the integrity of CLETS. In March 2019, NBC San Diego reported on a database that Customs and Border Protection “created a secret database of activists, journalists, and social media influencers.”⁸ Considering these reports, we have little faith that DHS and its component agencies will follow the PPP.

DOJ should initiate an audit of DHS and its component agencies, rather than relying on these agencies to investigate themselves, particularly because the agencies’ federal mandate runs counter to the California Values Act.

2. Enhanced Misuse Data Collection

After analyzing this year’s data and making calls to police agencies, EFF believes DOJ can make two simple changes to the misuse reporting form so that it better captures information about CLETS misuse.

DOJ’s improved process for collecting misuse data has resulted in a far greater percentage of agencies reporting misuse. While we are still waiting for a final tally for 2019, previous years indicate a rise from 58% compliance in 2017 to 98% compliance in 2018. By having more data, CAC and the public are able to better assess the scope of the problem of misuse.

A. DOJ Should Require Disclosure of the Number of Employees Who Committed Violations

The current misuse report does not capture context that would help DOJ and CAC better understand the severity and scope of CLETS misuse by agencies that respond. The report requires agencies to disclose the number of investigations conducted and then the number of found violations. But these are not a 1-to-1 comparison: one investigation may turn up

⁷ Srikrishnan, Maya. Voice of San Diego. “How California Laws Meant to Integrate Immigrants Can Open a Backdoor for ICE.” Feb. 19, 2019. Online: <https://www.voiceofsandiego.org/topics/news/how-california-laws-meant-to-integrate-immigrants-can-open-a-backdoor-for-ice/>

⁸ Jones, Tom; Mari Payton, and Bill Featuher. NBC San Diego. “Leaked Documents Show the U.S. Government Tracking Journalists and Immigration Advocates Through a Secret Database.” March 6, 2019. Online: <https://www.nbcsandiego.com/news/local/Source-Leaked-Documents-Show-the-US-Government-Tracking-Journalists-and-Advocates-Through-a-Secret-Database-506783231.html>

multiple examples of misuse. The number of misuse violations, however, does not indicate whether the problem was widespread or isolated.

For example, the Glendale Police Department (GPD) reported 15-25 violations in 2018. From the records, it is unclear whether this involved multiple or single individuals. If it were multiple individuals, it might require an evaluation of overall departmental culture. Upon calling Glendale, we learned that all violations were due to a single employee who decided to use CLETS to search for women he found attractive.

By comparison, the Chula Vista Police Department (CVPD) reported 38 violations in 2018, an all-time record. CVPD informed us that each violation was from multiple individuals. The violations, however, were all due to misunderstanding the rules for running background checks on retired peace officers seeking concealed weapons permits.

DOJ and CAC should add a new question to the misuse form that asks the agency to provide the aggregate number of how many individuals were found to have violated CLETS PPP. This would allow for greater context about misuse by an agency, particularly when large numbers appear in the data.

B. DOJ Should Require General Disclosure of the Nature of the Misuse

Because CLETS misuse reports do not require agencies to categorize the type of misuse they have identified, both DOJ and the public cannot fully understand the extent of any problems at a given agency. The Chula Vista Police Department data from this year's report is a good example of why DOJ should collect additional information about the type of misuse reported. A reader of the misuse data may conclude from CVPD's disclosure of 38 violations that the agency's misuse of CLETS poses a serious problem. In reality, it is an example of an agency identifying a problem in its training guidelines and disclosing these errors responsibly.

That same reader might also pay little attention to the Carlsbad Police Department, which only reported a single misuse case. However, this case was far more serious: a police officer had been charged with stalking an ex-partner and breaking into her home. In a phone call with EFF, Carlsbad Police explained that during the course of the internal affairs investigation, investigators found that the suspect had accessed CLETS in violation of the PPP days before his termination. Although the violation was unrelated to the domestic abuse allegations, it nonetheless resulted in a misdemeanor charge.

DOJ, CAC, and the public would benefit from an additional set of questions in which the agency discloses generally and in aggregate the nature of the violations. In its April 2018 information bulletin, DOJ lists several categories of potential CLETS misuse:⁹

- Querying yourself, a family member, friend, etc.

⁹ Information Bulletin on CLETS Misuse, *supra* note 1.

- Providing information from CLETS to another officer, individual, agency or company for unauthorized purposes
- Sharing user IDs or passwords
- Logging into CLETS and allowing others to utilize your authorized access
- Querying the Automated Criminal History System for licensing, employment or certification (such as Carry Concealed Weapon permits)
- Querying a firearm to determine if it is stolen prior to purchase
- Querying the Department of Motor Vehicles to obtain unauthorized address, vehicle registration, or insurance information
- Querying high profile individuals in the media

DOJ should require agencies to tally the nature of the abuse it reports under the categories it identified in the 2018 bulletin, and add any other categories it believes would be useful. By including this information, CAC would have more context for prioritizing which agencies should be evaluated for sanctions. The additional information would also let the public know how concerned it should be about the privacy practices in their local communities.

* * *

To conclude, we again applaud DOJ staff for its significant progress in addressing CLETS misuse. These advancements have strengthened the integrity of the public safety network and demonstrated the agency's commitment to transparency and accountability. Moreover, DOJ has shown that it is willing to engage with the public and EFF to address concerns about CLETS misuse.

Should you have further questions or responses, please do not hesitate to contact me by email at dm@eff.org or by phone at 415-436-9333 x 151. We would appreciate being kept informed about any further developments that improve the misuse reporting and investigation process.

Best regards,

Dave Maass
Senior Investigative Researcher
Electronic Frontier Foundation